DIR-DCS-MSI-MSA-001

Appendix 3 to the
Eleventh Amendment of
Master Services Agreement

May 31, 2016

Exhibit to Data Center Services Multisourcing Service Integrator Master Services Agreement

DIR Contract No. DIR-DCS-MSI-MSA-001

Between

The State of Texas, acting by and through
the Texas Department of Information Resources

and

Capgemini America, Inc.

Exhibit 2.1

Multisourcing Service Integrator (MSI)

Statement of Work

May 31, 2016

TABLE OF CONTENTS

A.0 SERVICE REQUIREMENTS 6
A.1.1 Service Desk 6
A.1.2 Incident Management 11
A.1.3 Problem Management 21
A.1.4 Change Management 30
A.1.5 Configuration Management 40
A.1.6 Release Management 47
A.1.7 Request Management and Fulfillment 50
A.2 Service Delivery Services 60
A.2.1 Availability Management 60
A.2.2 Capacity Management 65
A.2.3 Service Level Management 74
A.2.4 IT Service Continuity Management 74
A.2.5 IT Financial Management 81
A.2.6 Security Management 85
A.2.7 Vendor Management and Coordination 93
A.2.7.1 Service Component Management and Coordination 93
A.3 Equipment and Software Services 95
A.3.1 Long Range Planning 95
A.3.2 Evaluation and Testing 96
A.3.3 Refresh and Technical Currency 96
A.3.4 Service Catalog 98
A.3.5 Standard Products 99
A.3.6 Delivery and Staging 101
A.3.7 Equipment and Software Maintenance 101
A.3.8 Software Support 102
A.3.9 Administration 105
A.3.10 Redeployment and Disposal of Equipment 109
A.4 Other Services 110
A.4.1 Project Management and Support 110
A.4.1.1 Project Planning 111
A.4.1.2 Current and Ongoing Projects 112
A.4.1.3 Resource Rationalization 112
A.4.2 Quality Assurance 113
A.4.3 Operations Documentation 113

A.4.4 Additions, Mergers and other Reorganizations 113
A.4.4.1 Additional Customers 114
A.4.5 Crisis Management 115
A.4.6 Training and Education 115
A.4.6.1 Training for New Authorized Users 115
A.4.6.2 Ongoing Training for Authorized Users 116
A.4.6.3 Training for Service Provider Personnel 116
A.4.7 Portal 117
A.4.7.1 Document Data Store 118
A.4.8 Network Connectivity 119
A.5 Hybrid Cloud Initiative 120

EXHIBIT 2.1
MULTISOURCING SERVICE INTEGRATOR (MSI)
STATEMENT OF WORK

Update Methodology to Exhibit 2.1

The following update methodology is incorporated as part of **Exhibit 2.1**:

Title	Methodology for Updating Exhibit
Exhibit 2.1 Multisourcing Service Integrator Statement of Work	**Exhibit 2.1** may only be modified by formal amendment, in accordance with **Section 21.7** of the MSA.

Introduction

Service Provider will provide a solution that supports all of the business processes described in this Statement of Work and its Attachments, and that all Services, unless otherwise specifically stated, are included in the Base Charges.

Service Provider will be responsive to the current and future requirements of DIR and DIR Customers, by proactively anticipating needs, and adjusting Services accordingly within the Base Charges. Requirements for New Services will be handled in accordance with **Section 11.5** of the Agreement and Service Provider will work with DIR to assess the impact of these requirements on DIR's and DIR Customers' operating environment and supported Applications in accordance with the terms of the Agreement.

This Exhibit sets forth the Services that Service Provider will provide, as of the Commencement Date unless otherwise specified, for all Services that affect multiple Service Components described in this Exhibit.

Service Management

DIR bases its Service Management practices on the Information Technology Infrastructure Library (ITIL), a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. Accordingly, DIR requires that Service Provider's Service Management practices, which are used to support the Services, be based on the ITIL framework and guidance. The primary structure of the requirements in the Statements of Work are based on an ITIL v2 foundation with ITIL v3 guidance in select functional areas (e.g. Request Management and Fulfillment) with the expectation of migrating towards ITIL v3 progressively as process improvements are incorporated into the Service Management Manual.

Service Provider's responsibilities include:

1. Intentionally deploy and actively manage a set of Service support processes and Service delivery processes that are based on ITIL guidance to enable consistent management of

process-driven IT services seamlessly across a variable number of environments and among DCS Service Providers.

2. Ensure that ITIL-based processes effectively integrate with the processes, functions and roles deployed within and used by DIR and DIR Customers and other DCS Service Providers.
3. Execute detailed activities and tasks that are common to IT service operation and maintenance according to the guidance set out in the policies and procedures described in **Exhibit 2.1**, including the broader guidance provided regarding the ITIL-based Service Management processes.
4. Design processes and procedures to enable the effective monitoring and reporting of the IT services in a Multi-Supplier Environment.
5. Ensure that enterprise processes (e.g. Change Management, Configuration Management, Problem Management) are followed across the DCS Service Provider and Third Party Vendor(s) processes.
6. Coordinate the execution of all the processes across Service Provider, DIR, DIR Customers, and all Service Component Providers in order that all the individual components that make up the IT Services are managed in an end-to-end manner.

A.0 SERVICE REQUIREMENTS

All activities required to provide the Services set forth in this Statement of Work, including project-related support activities, are included in the Charges.

A.1 Service Support Services

A.1.1 Service Desk

Service Provider’s Service Desk shall be the single point of contact for Authorized Users regarding Incidents, which include events that cause or may cause an interruption or reduction of service, as well as for requests for information and requests for services relating to all of DIR’s and DIR Customers’ IT Services.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Integrate Service Provider’s Service Desk process with the Service Desk processes of other Service Component Provider(s), DIR Customer, and authorized Third Party Vendor(s), where the processes interact.
3. Integrate Service Provider’s Service Desk process with the other Service Management processes, including Incident Management, Problem Management, Change Management, Configuration Management and Service Request Management.
4. Coordinate Service Desk activities across all functions and organizations, including other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s), that provide services to DIR Customers.

5. Communicate and coordinate the Service Desk processes and policies within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

    5.1. Provide on-going methods for training Service Provider staff, other DCS Service Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Service Desk process and procedures.

6. Facilitate and lead in the definition and documentation of Service Desk Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Service Desk processes.

    6.1. Continually verify the effective compliance with the Service Desk Policies by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

7. Facilitate other Service Component Provider(s) support for Authorized Users on both a reactive and a proactive basis, and for both in-bound and out-bound support.

8. Manage all Incidents and Service Requests from Authorized Users relating to Services, including the following:

    8.1. Assigning categorization and prioritization codes.

    8.2. Communicating with users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Service Provider activities.

    8.3. Closing all resolved Incidents, Service Requests and other calls.

9. All communications, whether spoken or written, shall be clearly understandable to other Service Component Provider(s).

10. Seamlessly integrate the Service Desk — including tools, technology and processes — with the Service Desk(s) of other Service Component Provider(s).

11. Provide a Service Desk with processes for Service Delivery and Service Management that are ITIL-conformant, including the use of DIR and DIR Customer provided Service Desk attendant scripts for supporting incidents and service requests related to services, Applications, systems, etc.

12. Effectively implement and use the capability for Authorized Users to submit Incidents and Service Requests via email, a secure Web site, or other means approved by DIR.

    12.1. Routinely educate Authorized Users on the use of such means.

13. Analyze Incident trends, and recommend and implement actions, with DIR’s approval, to reduce Incidents, including:

    13.1. Increase the availability of self-help capability, such as through providing on-line FAQs and help documentation for common problems across Service Desks.

    13.2. Keep Authorized Users regularly updated with alerts advising of any new or changed information.

    13.3. Collate Incident information from Authorized Users regarding suggested improvements to Service Provider’s service.

13.4. Develop an Action Plan on a quarterly basis to address these suggested improvements.

13.5. Review the Action Plan for DIR's approval.

13.6. Report on progress and improvements made.

14. Conduct random surveys of Authorized Users immediately after they have used the Service Desk in accordance with the Service Management Manual and Customer Satisfaction Survey requirements, and report the results to DIR each month.

15. Develop and periodically update Incident and Problem escalation procedures, and distribute such procedures to designated Authorized Users upon DIR's review and approval.

16. Develop and document processes regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either submit an Incident or receive an Incident.

A.1.1.1 General Service Desk

Service Provider's responsibilities include:

1. Provide support to Authorized Users on both a reactive and a proactive basis, and for both in-bound and out-bound support.

1.1. Provide process to handle designation and establishment of Authorized User rights.

1.2. Track and manage the rights associated with individual Authorized Users.

2. Manage all Incidents and/or Service Requests from Authorized Users relating to Services, including the following:

2.1. Logging all relevant details.

2.2. Providing first-line investigation and diagnosis.

2.3. Resolving those as possible.

2.4. Escalating those that cannot be resolved within agreed timescales.

2.5. Communicating with users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Service Provider activities.

2.6. Making appropriate updates to the Configuration Management System (CMS) in compliance with Configuration Management processes.

3. Ensuring staffing levels and work allocation remains appropriate to handle incident volumes and incident response targets.

4. Ensure that the Service Desk is available at all times (i.e. 24 hours a day, 365 days a year).

5. Provide an effective means of using industry recognized methods to determine, measure and monitor staffing levels, requirements and allocations, including the use of the following considerations:

5.1. Customer service expectations.

5.2. DIR and DIR Customer business requirements.

5.3. Size, relative age, design and complexity of the IT Infrastructure (e.g. the number and type of incidents, the extent of customized versus standard deployments).

5.4. The number of DIR Customers and Authorized Users to support, and associated factors such as number of customers, language requirements and skill level.

5.5. Incident and Service Request types, including duration of time required for call types, local or external expertise required, the volume and types of incidents and Service Requests.

5.6. The period of support cover required, based on hours covered, out-of-hours support requirements, time zones to be covered, locations to be supported, workload pattern of requests, and the service level targets in place.

5.7. The type of response required (e.g. telephone, email, fax, voicemail, physical).

5.8. The level of training required.

5.9. The support technologies available (e.g. phone systems, remote support tools, etc.).

5.10. The existing skill levels of staff.

5.11. The processes and procedures in use.

6. Communicate to Authorized Users in English, using terms that are clearly understood by the Authorized Users and consistent with those used by DIR.

6.1. All communications, whether spoken or written, shall be clearly understandable to the Authorized User.

7. Seamlessly integrate the Service Desk — including tools, technology and processes — with DIR Customer IT Service Desk(s).

8. The Service Desk will be located in an off-site location from DIR (approved by DIR), except for temporary periods where:

8.1. Calls are overflowed from one team within the Service Desk to another to handle major outages and business releases.

8.2. Calls that overflow to a different team within the Service Desk are handled by Service Desk personnel who have been trained and are knowledgeable on the DIR and DIR Customer environment.

8.3. Where more than one site is proposed for the delivery of Service Desk Services, any switching between the sites must be transparent to Authorized Users.

9. Provide Service Provider Service Desk personnel that are trained for the following:

9.1. Possess the appropriate competencies to provide Service Desk Services.

9.2. Understand DIR’s business, service levels, and its customers and respond appropriately.

9.3. Understand DIR’s and DIR Customers’ technology and sourcing arrangements.

9.4. Use recognized customer service and interpersonal skills, such as telephony skills, communication skills, active listening and customer care training.

9.5. Make appropriate decisions and initiate actions that reflect DIR and DIR Customer priorities.

9.6. Understand changes in products and services, as they become part of Service Provider's responsibilities.

10. Provision Service Desk Support on a 24x7 basis.

11. Provide a single, toll-free (in-country) telephone number for external calls to the Service Desk from Authorized Users.

12. Provide DIR with an alternative local number (in-country) for calls to the Service Desk.

13. Identify potential Authorized Users' training requirements, and provide recommended training actions to DIR.

14. Provide and maintain instructions for Authorized Users to access the Services.

14.1. The instructions will be made available to Authorized Users via the Portal and other media as requested by DIR.

A.1.1.2 Service Desk Knowledge Management

Service Provider's responsibilities include:

1. Provide and routinely update a list of FAQs regarding the Services on the Portal.
2. Publish answers to the FAQs using a media that is efficient, easy to use, and easily accessible for Authorized Users, as well as subject to approval by DIR.
3. Compile lists of FAQs where recommended solutions can be made available to Authorized Users to increase Authorized Users' ability to Resolve Incidents and handle Service Requests.
4. Publish FAQs lists for DIR and DIR Customers.
5. Provide FAQs in a format that can easily be published on DIR's and DIR Customers' internal systems.

A.1.1.3 Service Desk Management Reporting

Service Provider's responsibilities include:

1. Provide regular reports to DIR on Service Desk activities and performance, which at a minimum includes:

1.1. Key issues relating to Service Desk processes, improvements, script development.

1.2. Status as to Service Desk staffing, training, and authorization.

1.3. Integration activities and issues with other Service Desks belonging to DIR, DIR Customers and other Service Component Providers as directed by DIR.

1.4. Trend analysis during the thirteen (13) most recent months.

1.5. Calculate metrics and provide monthly reports to DIR, to at least include:

1.5.1. Number of Contacts, to include all Calls, phone calls, electronic, automated or otherwise.

1.5.2. Number of calls abandoned, average call duration, average time to answer, average time to abandon.

1.5.3. Number and percentage of Contacts resolved.

1.5.4. Number and percentage of Contacts passed to other Service Desks.

1.5.5. Other pertinent information regarding Service Desk operation and performance.

A.1.2 Incident Management

Service Provider's Incident Management discipline shall encompass Incident Management processes deployed across all Service Components that are designed to: restore service as quickly as possible, minimize disruption to DIR Customer businesses, aim for best levels of availability and service quality, completely transparent and auditable delivery of service, and promote the highest level for user satisfaction.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Incident Management.
3. Validate that the Incident Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Designate end-to-end responsibility to a single Service Provider and ownership for each Incident to a single Service Provider staff member, thus minimizing redundant contacts with the Authorized User.
5. Integrate Service Provider's Incident Management process with the Incident Management processes of other Service Component Provider(s), DIR Customers, and authorized Third Party Vendor(s), where the processes interact.
6. Integrate Service Provider's Incident Management process with the other Service Management processes, including Problem Management, Configuration Management, Service Level Management and Change Management.
7. Coordinate Incident Management activities across all functions and organizations, including other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s), that provide services to DIR Customers.
8. Communicate and coordinate the Incident Management processes and policies within Service Provider's own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

   8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Incident Management process.

   8.2. Regularly provide guidelines, FAQs and access to appropriate tools to other Service Component Provider(s), DIR, DIR Customers and authorized Third Party

Vendors to promote and reinforce the appropriate use of Incident and escalation procedures.

9. Facilitate and lead in the definition and documentation of Incident Management Policies and Procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Incident Management processes.

    9.1. Routinely verify the effective compliance with the Incident Management Policies and Procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

10. Provide effective and agreed mechanisms for properly establishing the priority of incidents based on established prioritization criteria (e.g. scripts, diagnostic tools, etc.).

11. Prioritize and escalate Incidents from VIP or Executive Users or as authorized by DIR and DIR Customers.

12. Link multiple Contacts pertaining to the same Incident to the associated Incident Record.

13. Link multiple Incidents pertaining to the same (Incident) to the associated (Incident).

14. Review completeness of incident (e.g. work detail notes) and perform a management review by Service Component every week and report accordingly.

15. Close an Incident, including Service Requests, after receiving confirmation from the affected Authorized User, or Service Provider support personnel for incidents reported via an event detection tool, that the Incident has been Resolved.

    15.1. Follow Service Management Manual guidelines for closure where Authorized Users confirmation has not been received.

    15.2. Close master Incident only after all related tickets have been closed.

16. Retain overall responsibility and ownership of all Incidents until the Incident is closed subject to DIR Customer approval.

17. Track and report the progress of Resolution efforts and the status of all Incidents, including:

    17.1. Review the proposed Resolution time for each Incident with the appropriate party and update the status accordingly.

    17.2. Coordinate Incident tracking efforts, and provide and maintain regular communications, per the Service Management Manual, between all parties and Authorized Users until Incident Resolution.

    17.3. Keep DIR and DIR Customer informed of changes in Incident status throughout the Incident life cycle in accordance with agreed Service Levels.

    17.4. Keep DIR Customer informed of anticipated Resolution times for active Incidents.

18. Provide for training on processes and tools for Incidents and escalations to:

    18.1. End-User training to authorized users within DIR and DIR Customers.

    18.2. Other Service Component Provider(s) and authorized Third Party Vendors as specified by DIR and DIR Customers.

    18.3. Service Provider Incident Management staff and other relevant resources involved with responding to Incidents.

A.1.2.1 General Incident Management

Service Provider’s responsibilities include:

1. Provide an Incident Management process that will restore service operation as quickly as possible with minimum disruption to the business, thus enabling the best achievable levels of availability and service quality to be maintained to promote Customer and Authorized User satisfaction.
2. Manage the effective execution of Incident Management to achieve its primary purpose to restore service as quickly as possible with minimal business impact.
3. Implement an Incident Management process that is flexible and facilitates effective communication and coordination across functions, DIR and DIR Customer Sites, regions and Third Party Vendor(s).
4. Record detailed audit trail information of all activity that creates, changes, or deletes data and user access to all systems that contain DIR and DIR Customer data.
5. Communicate the Incident Management process to Service Provider’s organization and each Third Party Vendor(s) involved in the delivery of Services.
6. Where an Operational Level Agreement (OLA) does not exist, proactively work with Service Provider, DIR, DIR Customers and/or Third Party Vendor(s) to deliver the Services required.
7. Develop and document processes and procedures regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may either raise an Incident, receive an Incident, or support the Resolution of Incidents.
8. Provide a mechanism for handling of Incidents according to the agreed to prioritization model used by DIR, DIR Customers, and Third Party Vendor(s), based on the assigned Severity Level, in compliance with the Incident Management and Problem Management Processes described in the Service Management Manual.
9. Provide a mechanism for expedited handling and increased communication of Incidents that are of high business priority to DIR, DIR Customers, and Third Party Vendor(s), based on the assigned Severity Level, in compliance with the Escalation Processes described in the Service Management Manual.
10. Integrate with other DCS Service Provider(s) and Third Party Vendors who provide IT services to DIR and DIR Customers in order to provide real-time visibility of data records associated with Incidents, including Service Requests to DIR, DIR Customers, and other Third Party Vendors.
11. Develop, utilize, manage and continually improve an inventory of defined and documented Incident models that incorporate at a minimum the following elements:
    - 11.1. Sequences of tasks, actions or steps to execute the Incident model and resolve the Incident.
    - 11.2. Identification of required dependencies, data sources, etc. that must be considered in executing the Incident model.
    - 11.3. Definition of responsibilities and roles to execute the Incident model.
    - 11.4. Timescales, milestones and thresholds for executing the Incident model.

11.5. Anticipated escalation points and escalation procedures associated with the Incident model.

11.6. Tasks, activities, methods, tools, systems, etc. to ensure that detailed audit information be recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DIR Customer data.

12. Initiate Problem Management as appropriate and at a minimum when:

12.1. The service is still interrupted, and a workaround is not available;

12.2. The root cause of the Incident has not been identified;

12.3. Multiple occurrences of an Incident warrant a Root Cause Analysis; or

12.4. DIR or DIR Customer request (see Problem Management).

13. Provide effective training on the purpose, activities, procedures, tools, policies, interfaces, etc. for all stakeholders to ensure effective execution of the process.

14. Provide additional treatment of Major Incidents as required.

A.1.2.2 All Incidents

Service Provider’s responsibilities include:

1. Receive and record all Incidents (including submissions received by telephone, electronically, or other means approved by DIR) in an Incident Record or Service Request Record as appropriate, including classification and initial support.
2. Enable Incident detection by DCS Service Providers (including links to event monitoring tools), reporting, recording, classification and initial support.
3. Provide Incident investigation, diagnosis, impact analysis, and reclassification as required.
4. Utilize and update the Incident Management System with all relevant information relating to an Incident within the designated time and in a complete manner.
5. Make an initial determination of the potential Resolution and document in the Incident Management System.
6. Resolve Incidents requiring Level 1 Support and close after receiving confirmation to close from the affected Authorized User, or Service Provider support personnel for Incidents reported via an event detection tool.
7. Ensure resolution of Incidents arising from or related to the Services, including break/fix Hardware and Software support.
8. Act proactively, and coordinate with all other third parties to Resolve Incidents and action Service Requests in a way that ensures effective coordination and avoids conflict of resource allocations, control objectives, etc.
9. Transfer Incidents within specified time limits to the appropriate party without compromising Service Levels or security requirements.
10. Ensure that proper escalation and prioritization policies and procedures are properly managed to ensure that incident response and resolution is handled within the intents and guidelines of the prioritization model agreed to.

11. Provide or coordinate the final Resolution including Service Request Management.

12. Ensure proper testing of incident resolution responses to ensure effective resolution and closure of the incident while avoiding / minimizing (unintended) impact to the customer / user.

13. Escalate issues to the appropriate levels/functions for Resolution in accordance with escalation procedures approved by DIR.

14. Escalate an Incident where the Incident cannot be Resolved within the relevant Service Levels or agreed timeframe.

15. Ensure consistent ownership of the Incident from recording to Resolution.

16. Record all information on the details of the Incident and the corrective action for later statistical analysis.

17. Create an audit trail of all activity that creates, changes, or deletes data and user access to systems that contain DIR Data and preserve end-to-end traceability across Applications, systems, and parties.

18. Review incidents prior to closure to ensure proper categorization, documentation, confirmation of resolution and activities required to initiated appropriate actions / processes (e.g. configuration information updates, creation of problem records, etc.).

    18.1. Review Incident Record(s) to show the proper Root Cause Analysis classification.

    18.2. Review Incident Record(s) to show all Authorized User interactions, including all customer notifications, customer agreement as to closure, and customer agreement as to classification prior to closure.

    18.3. Review Incident Record(s) to assure that associated Incidents, such as duplicate Incidents, are properly noted to preserve complete and accurate record.

19. Restore normal service operations as quickly as practical following an Incident, with minimum disruption to DIR’s and DIR Customers’ business operations, and in compliance with Service Levels.

20. Leverage a knowledge base as part of Operational Documentation requirements in Section A.4.3 of this **Exhibit 2.1** to assist with the Resolution of Incidents and the processing of Service Requests, including:

    20.1. Make the knowledge base available on the Portal to Authorized Users for user self-help.

    20.2. Track the use of the knowledge base and report usage statistics to DIR on a monthly basis, or as requested by DIR (i.e. the number of Incidents Resolved using the knowledge base).

21. Where Incidents relate to the move of Assets, update in all relevant configuration management systems (e.g. CMS / CMDB), or coordinate with the relevant process to confirm updates are made.

22. Where Incidents result in a Change in the IT environment, Service Provider shall initiate and manage such Changes through the Change Management process as appropriate.

23. Where Incidents require the changing of software or hardware assets submit a request for change through the Change Management Process and update the Definitive Media Library (DML) or coordinate with the relevant process to confirm updates are made.

A.1.2.3 Incidents Only Partially Related to Services

Service Provider's responsibilities include:

1. Continue to work toward Resolution of the portion of the Incident relevant and related to Services, in compliance with All Incident processes, the Service Management Manual and within agreed Service Levels.
2. Transfer the remaining part(s) to DIR, DIR Customer, or other Third Party, without compromising Service Levels.
3. Record the Incident or other tracking information provided by DIR, DIR Customer, or other Third Party.
4. Record contact information of other parties as appropriate to ensure appropriate follow-up and facilitate auditing (e.g. names, phone numbers, emails, etc.).
5. Communicate status updates to DIR Customers and Authorized User in compliance with the Service Management Manual and within agreed Service Levels.

A.1.2.4 Major Incidents

Service Provider's responsibilities include:

1. Develop and document the standard process for managing Major Incidents (the highest level of prioritization according to the agreed prioritization model) from identification through closure.
2. Provide identification and assignment of the Incident (and the execution of the applicable processes) to an Incident Manager that provides an appropriate level of dedicated attention to the incident.
3. Formulate a team (scoped as appropriate to the type of incident) to work under the direct leadership of the Incident Manager, in order to concentrate on this incident alone to ensure that adequate resources and focus are provided to finding a swift resolution.
4. Establish and provision any supporting communication facilities (i.e. conference bridges, on-line work spaces, etc.) that may be required to support the effective facilitation of Incident diagnosis and resolution.
5. Provide management and control of the Incident from identification to resolution, including the following:
    - 5.1. Review the proposed Resolution time for each Incident with the appropriate party and update the status accordingly.
    - 5.2. Coordinate Incident tracking efforts, and provide and maintain regular communications between all parties and Authorized Users until Incident Resolution.
    - 5.3. Keep DIR and DIR Customer informed of changes in Incident status throughout the Incident life cycle, in accordance with Service Levels.
    - 5.4. Keep DIR Customer informed of anticipated Resolution times for active Incidents.

A.1.2.5 Incident Escalation

Service Provider's responsibilities include:

1. Provide a process for escalating to Service Provider's management, Incidents not Resolved in the time frames appropriate to the severity of the Incident and the priority of the user.
2. Provide process and procedures for DIR, DIR Customers and other Service Component Provider(s) to escalate Incidents.
3. Define and maintain Incident escalation procedures in the Service Management Manual.
4. Escalate Incidents according to processes and procedures approved by DIR, and documented in the Service Management Manual.
5. Automatically prioritize high-impact Incidents, as defined by DIR such that they are treated with the highest priority.
6. Provide for emergency escalations to authorized tier-2 suppliers, Third Party Vendors and other Third Party Resources by and at the discretion of DIR.
7. Implement escalation processes and procedures that reflect and describe at a minimum the following items:
   - 7.1. Severity Level of the Incident.
   - 7.2. Impact on affected Users (e.g. location of the Incident, names and/or number of users).
   - 7.3. Priority of the User (e.g. Executive Director, Legislative request, etc.).
   - 7.4. Elapsed time before an Incident is escalated for Resolution as if it were the next higher Severity Level.
   - 7.5. The levels of involvement (and notification), for escalation of incidents, of Service Provider management and DIR and DIR Customer management at each Severity Level.
   - 7.6. Investigative and diagnostic activities to identify temporary workarounds for each Incident.
   - 7.7. Incident Resolution activities to restore normal service in compliance with the Service Levels.
   - 7.8. Ability to Resolve Incidents by matching Incidents to known errors that are stored in a Known Error Database.
   - 7.9. Ability to Resolve Incidents by implementing workarounds that are stored in a Known Error Database.
   - 7.10. Process used to escalate Incidents to appropriate support teams when necessary.
   - 7.11. Process used to escalate Incidents to Service Provider's management team and/or DIR's and DIR Customers' management team.
8. Track information regarding escalations to include frequency of usage by DIR Customers.

A.1.2.6 Incident Management System

Service Provider will utilize an Incident Management Systems that provides a level of sophistication that allows for a set of Incident Resolution diagnostics and will track Software and Equipment to enable the automation of monitoring, detection, prioritization, establishment of resolution times and the Resolution of Incidents associated with the Services.

Service Provider's responsibilities will include:

1. Implement an automated Incident Management System, including the integration of applicable software, equipment, email, telephony, and Web technologies.

    1.1. Provide access to the Incident Management System to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors, including all appropriate and required licenses and/or interfaces.

2. Maintain a central knowledge database used to capture, store, and retrieve information and solutions for reuse by Service Provider personnel, other Service Component Provider(s), authorized Third Party Vendor(s), and Authorized Users.

    2.1. This central knowledge database shall enable the sharing of policies, procedures, best practices, and methods to Resolve Incidents among Service Provider personnel, other Service Component Provider(s), authorized Third Party Vendors(s), and Authorized Users.

3. Integrate with other Service Management Systems, including Problem Management, Configuration Management, Service Level Management, Change Management and Release Management.

4. Integrate with the Incident Management Systems of other Service Component Provider(s) and designated Third Party Vendors.

    4.1. Enable interfaces to integrate with other Incident Management systems of other Service Component Provider(s), DIR, DIR Customers and authorized Third Party Vendors, as directed by DIR.

    4.2. Provide customizable capability that allows different configurations of interfaces based on standard user profiles.

5. Grant DIR and DIR Customers access to the database of the Incident Management System, and allow DIR and DIR Customer to monitor and view on an ongoing basis.

6. Limit access to the Incident Management Systems to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

7. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the Incident Management System.

8. The Incident Management System shall:

    8.1. Securely segregate DIR and DIR Customer data so that it can be accessed only by those authorized to comply with Government security requirements and in accordance with DIR policy.

    8.2. Provide for the partitioning of DIR Customer information in management and reporting.

8.3. Provide for granting additional access in support of other Authorized Users (e.g. Audits) upon the request and as directed by DIR.

8.4. Provide information necessary to record Incidents, track Incidents, and support Incident Management for each Incident submitted to (or originating from) the Service Desk, including, at a minimum:

8.4.1. Incident Identifier

8.4.2. Category (based on required categorization schema agreed with DIR and DIR Customer)

8.4.3. Prioritization (including impact and urgency, based on required prioritization schema agreed with DIR and DIR Customer)

8.4.4. Reported by (person, system, etc.)

8.4.5. Method of notification

8.4.6. Issues experienced, symptoms of incident, etc.

8.4.7. Action taken to diagnose and resolve Incident

8.4.8. Cause and resolution by Service Component

8.4.9. Incident open date/time

8.4.10. Outage or Downtime start /end

8.4.11. Incident close date/time

8.4.12. Escalation details

8.4.13. Other information as needed to support the Service Level metrics

8.4.14. Other information as needed to support reporting or as requested by DIR

8.5. Identify Authorized Users designated by DIR and DIR Customer.

8.6. Capture data pertaining to volumes to include Incident types by hour per day; Service Desk call abandonment, telephone call queue lengths, and time-to-answer rates for telephone calls; and time-to-log for email, facsimile, and Web-based Incidents.

8.7. Provide for logging all modifications to Incident Records, to provide full tracking, audit trail and change control at the named-user level.

8.8. Provide functionality to manage information for each Incident submitted to, and originating from, Service Provider.

9. Provide online reporting capability with reasonably current data (and with unrestricted query length and depth) for use by Authorized Users in the generation of sophisticated, custom reports.

10. Provide end-to-end traceability, even when transactions span across multiple Applications, systems components, or parties.

A.1.2.7 Incident Management Notifications

Service Provider’s responsibilities include:

1. Provide regular progress notifications to DIR and DIR Customers on current Incidents for all Severity Levels.
   1.1. The frequency of such notification shall be determined by the severity of the Incident as determined using the definitions given in **Attachment 3-E**.
2. Provide prompt notification to DIR and DIR Customer of system outages on critical systems identified in the Incident Management System; and otherwise provide affected Authorized Users with regular progress updates within designated timeframes, as prescribed in the Incident Management notification section of the Service Management Manual, that clearly indicate the following:
   2.1. Nature and scope of the Incident.
   2.2. Estimated time to completion.
   2.3. Potential short-term alternatives.
3. Maintain communications and provide status reports to DIR and DIR Customer, Service Desk and appropriate Third Party Vendor(s) from the time an Incident is identified through Resolution, and, as necessary, through any follow-up communication and work required post-resolution as defined in the Service Management Manual.

A.1.2.8 Incident Management Reporting

Service Provider’s responsibilities include:

1. Provide reports on compliance with Service Provider ability to record detail audit trail information, as requested by DIR and DIR Customers.
2. Provide monthly report(s) in electronic copy to DIR and DIR Customers, in the DIR approved format, which at a minimum includes:
   2.1. Key issues relating to Incident Management processes.
   2.2. Number of Incidents during the month, grouped by severity, service, agency, region, classification or other criteria as appropriate.
   2.3. List of Incidents, short description, reference number, and a shortcut to detailed description.
   2.4. Detailed description, including timing of activities.
   2.5. Links to Problems and Known Errors.
   2.6. Trend analysis of the Incidents reported during the thirteen (13) most recent months.
   2.7. Calculate metrics and provide monthly reports to DIR and DIR Customers, which include:
      2.7.1. The number of Incidents.
      2.7.2. Sources of the Incidents.
      2.7.3. Frequency regarding the types or categories of Incidents.
      2.7.4. The duration of open Incident (average and quantities by age).
      2.7.5. Number and percentage of Incidents Resolved upon first contact.

2.7.6. Trending metrics in terms of MTTRS (mean time to restore service) by category, priority and by service or SLA.

2.7.7. Number and percentage of SLA impacting Incidents.

2.7.8. Number and percentage of Incidents (by category, priority, service and SLA) that were handled within the SLA targets.

2.7.9. Number and percentage of Incidents (by category, priority, service and SLA) reopened.

2.7.10. Number and percentage of Incidents (by category, priority, service and SLA) reoccurring.

2.7.11. Number and percentage of Incidents that have resulted in the creation of problem records.

2.7.12. Percentage (by category, type and priority) of Incidents that were resolved by use of an Incident Model;

2.7.13. Number and percentage of Incidents escalated by organization, category, priority and Service.

2.7.14. The association of Incidents by cause and resolution by Service Component.

2.7.15. Other pertinent information regarding Incident Resolution, including Service Level measurement reporting.

A.1.3 Problem Management

The Problem Management Process will minimize the adverse effect on the business of Incidents and Problems caused by errors in the IT infrastructure, Applications, systems and supporting components, and will proactively prevent the occurrence of Incidents and Problems by identifying and eliminating causes of failure.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Problem Management.
3. Enable the integration of other Service Component Provider(s) to the Problem Management process.
4. Integrate Service Provider’s Problem Management process with the Problem Management process of other Service Component Provider(s), DIR, DIR Customers, and Third Party Vendor(s), where the processes interact.
5. Integrate Service Provider’s Problem Management process with the other Service Management processes, including Incident Management, Availability Management, Configuration Management, Service Level Management, Change Management and Release Management.

6. Communicate and coordinate the Problem Management Process within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

    6.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Problem Management Process.

7. Facilitate and lead in the definition and documentation of Problem Management Policies, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Problem Management processes.

    7.1. Routinely verify the effective compliance with the Problem Management Policies by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

8. Effective execution of Root Cause Analysis.

9. Conduct regularly scheduled Problem Management meetings to prioritize the Resolution of Problems across other Service Component Provider(s).

    9.1. Document and publish Problem Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Providers and authorized Third Party Vendors.

10. Provide means for Problem records to be created from all relevant sources, specifically including the following:

    10.1. Staff of Service Provider.

    10.2. The Service Desk.

    10.3. Incident Management processes and Incident Management System.

    10.4. Event Monitoring systems and tools.

    10.5. Other Service Component Provider(s) and authorized Third Party Vendors.

    10.6. The systems development and release processes.

    10.7. DIR and DIR Customers.

    10.8. Root Cause Analysis reporting.

11. Track requests for Problem Management initiation, by source, organization and Authorized User.

12. Provide a means for prioritizing Problems / Known Errors based on considerations of business impact, urgency and severity using the prioritization model agreed to and approved by DIR and which aligns with the method for prioritizing Incidents.

13. Provide a means for categorizing Problems / Known Errors using the categorization model agreed to and approved by DIR and which aligns with the method for categorizing Incidents.

14. Implement a Problem Management System, including the integration of systems and processes of other Service Component Provider(s).

    14.1. As part of the Problem Management System, provide a Known Error Database or Knowledge Database that will be used for storing knowledge, records and information regarding previous Problems, Known Errors, workarounds and incidents (including both diagnostic and Resolution information), and which will be available for use by all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.

15. Train all relevant stakeholders in the use of the Problem Management System and Known Error Database / Knowledge Database.
16. Coordinate Problem tracking efforts and notifications to the Service Desk and Third Party Vendor(s) and maintain regular communications between all parties until Problem Resolution.
17. Retain overall responsibility and ownership of all Problems until the Problem is closed subject to DIR Customer approval.
18. Conduct Major Problem Reviews associated with all Major Incidents that arise or may arise out of the Services.

    18.1. Coordinate all communications and notices for Major Problem Reviews to all relevant stakeholders, including other Service Component Provider(s), DIR, DIR Customers, and in compliance with the processes in the Service Management Manual.

A.1.3.1 General Problem Management

Service Provider’s responsibilities include:

1. Implement a robust and auditable process for Problem Management, which is approved by DIR.
2. Use the approved Problem Management process to reduce the recurrence of Incidents.
3. Communicate the Problem Management process within Service Provider and to each Third Party Vendor(s) with which an OLA or underpinning contract exists.
4. Manage the effective entry of data into Problem Management systems and escalate to DIR and DIR Customer for prioritization and approval.
5. Manage and Resolve any deviation from the effective management of Problems.
6. Perform regular review of Incidents to identify recurring Incidents and associated Problems.
7. Engage with Financial Management processes to provide effective business cases / return on investment analysis to quantify the cost and benefit of implementing Problem / Known Error Resolutions.
8. Implement the corrective actions as identified in an expedited fashion.
9. Submit Request for Changes (RFC) through the Change Management Process to request the Resolution of Problems / Known Errors.
10. Validate that Problem Resolution and corrective actions taken through Change Management are sufficient to confirm that root causes identified do not recur in same or similar environments. This includes update of manuals, procedures, and other documentation, and the submission of RFCs through the Change Management process to facilitate changes to other services, systems or components which have been impacted by the same or similar Problems / Known Errors.

11. Verify and track that the identified corrective actions are being implemented.
12. Escalate to appropriate management within DIR, DIR Customers, Service Provider and all Third Party Vendor(s) if corrective actions are not being closed.
13. Document workarounds for Incidents that can be used to support the handling of future Problems and Incidents, and which will:
    - 13.1. Be stored in the Known Error Database / Knowledge Database.
    - 13.2. Have a unique identifier or reference number.
    - 13.3. Be categorized in a manner like the categorization of Incidents and Problems in order to facilitate effective identification and use.
    - 13.4. Provide a detailed description of the steps to be executed to implement the workaround.
    - 13.5. Provide a detailed description of any required inputs, capabilities, resources, etc. that are required for proper execution of the workaround.
    - 13.6. Describe the appropriate context under which the workaround is to be used and/or conditions under which it is not to be used.
    - 13.7. Provide a reference to previous Incidents, Problems and Known Errors to which the workaround is related.
    - 13.8. Provide a reference to the service, system or configuration item / component to which the workaround is related.
14. Update Known Error Database / Knowledge Database with all relevant information, including documented workarounds for Problems / Known Errors as they identified and addressed.
15. Routinely perform trend analyses on the volume and nature of Problems in order to identify areas for improvement.
16. Provide additional treatment of Major Problems as required.
17. Develop tools/scripts and enhance processes to proactively perform Problem Management, with the objectives of automating the Problem Management process and predicting Problems before they occur.
18. Implement measures to avoid unnecessary reoccurrence of Problems.
19. Manage all Problems in accordance with consistent and agreed classification and prioritization criteria.

A.1.3.2 Major Problem

Service Provider’s responsibilities include:

1. Effectively execute Major Problem Reviews associated with all Major Incidents that arise or may arise out of the Services, in compliance with the processes defined in the Service Management Manual.
    - 1.1. The assignment of a Problem Manager to facilitate the Major Problem Review.
    - 1.2. An analysis of lessons learned from the Major Incident (e.g. things done well, things needing improvement, etc.).

1.3. A description of the associated Incident, including description of the failure, business impact, duration, affected systems, affected services, affected customers, work executed to Resolve the Incident, etc.

1.4. A detailed Root Cause Analysis of the Incident.

1.5. Identification of any Problem / Known Error records and/to workarounds associated with or created.

1.6. Communication of findings and outcomes to all relevant stakeholders.

1.7. The identification, documentation and submission of identified improvements.

1.8. Preventive action items tracked to completion, including regular communication with relevant stakeholders during the process.

1.9. Notice to all relevant stakeholders when preventative action items have been completed or missed.

A.1.3.3 Root Cause Analysis

Service Provider's responsibilities include:

1. Effective execution of Root Cause Analysis (RCA) in compliance with the processes defined in the Service Management Manual.
2. Provide for an RCA Coordinator to act as the day-to-day interface into the RCA process.
3. Initiate RCA for all Incidents not resolved within Service Levels.
4. Provide a process for DIR and DIR Customers to request an RCA.

   4.1. Track all such requests and provide status.
5. Assign RCAs to a specific RCA Analyst to facilitate data gathering, interviews, analysis, and formulation of report.
6. Ensure that all appropriate roles are engaged to perform RCA tasks.
7. Document the RCA activity and outcomes in records associated with Problems, Known Errors, workarounds and Major Problem reviews, including the following at a minimum:

   7.1. Identification of associated Problem / Known Error record.

   7.2. Details of action taken to analyze the Root Cause, including details regarding the use of standard problem analysis tools.

   7.3. Details of findings from analysis of Root Cause.

   7.4. Details of business impact resulting from the Root Cause.

   7.5. Details regarding all services, systems, components, etc. effected by the Root Cause.

   7.6. Details regarding any considerations that should be included in business cases and cost benefit analyses.

   7.7. Provide tracking and reporting of RCA actions to completion.
8. Track open RCAs and identify any RCA that requires increased focus to meet committed service levels.

9. Accomplish Root Cause Analysis, as documented in the Service Management Manual, and which should include processes for:
    9.1. Addressing the primary root causes of Problems
    9.2. Investigating and identifying the root cause of the Problem in order to transform the Problem to a Known Error.
    9.3. Take all available information for a Problem Resolution, analyze it, formulate a hypothesis of the actual cause, promote peer review, adjust as needed, and finally close the acceptable investigation.
    9.4. Minimize the duration of Problems.
    9.5. Reduce the number of Problems.
    9.6. Minimize Problem life cycles.
    9.7. Optimize time and effort spent resolving Problems.
    9.8. Identify and address any contributing factors which increased the duration of the outage.
    9.9. Prevent recurrence of Incidents and Problems.
    9.10. Identify, address and implement all possible and reasonable preventive actions to permanently resolve the Problem and any contributing factors to prevent recurrence.
    9.11. Providing useful information about root causes to increase the rate of first-contact Resolution of Incidents.
    9.12. Supporting proactive Problem handling.
    9.13. Providing information related to service level violations.
    9.14. Managing RCAs within agreed times.
10. Assisting in reassignment of misdirected RCAs.
11. Maintain the quality and accuracy of the RCA information.
12. Provide processes for Service Provider, DIR, DIR Customer, and designated Third Parties to escalate non-performing RCA, as required to bring the Resolution of the RCA back on schedule.
13. Provide RCA-related education to Service Provider personnel, DIR, DIR Customers and designated Third Party Vendors.
14. Provide RCA reporting as documented in the Service Management Manual, and which should include processes for:
    14.1. Providing a preliminary report to DIR and DIR Customers as soon as possible.
    14.2. Providing a standard electronic report on RCAs.
    14.3. Presenting a final RCA to DIR and DIR Customers as required.

A.1.3.4 Problem Management System

Service Provider’s responsibilities include:

1. Implement an automated Problem Management System and Known Error Database, including the integration of applicable Software, Equipment, communications, and databases.

   1.1. Provide access to the Problem Management System, including the Known Error Database, to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors, which access shall include all appropriate and required licenses and/or interfaces.

2. Integrate with Service Provider’s other systems, including Incident Management, Configuration Management, Service Level Management, Change Management and Release Management.

3. Enable data exchange between the Problem Management Systems and the problem management systems of other Service Component Provider(s) and designated Third Party Vendors, as directed by DIR.

4. Limit access to the Problem Management Systems to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

5. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the Problem Management System and Known Error Database.

6. Grant DIR access to the database(s) of the Problem Management System, including the Known Error Database, and allow DIR and DIR Customer to monitor and view on an ongoing basis.

7. The Problem Management System shall include at a minimum the following:

   7.1. Functionality to manage information for each Problem submitted to, and originating from, Service Provider.

   7.2. A sophisticated set of problem resolution, diagnostic, and tracking Software and Equipment to enable the automation of monitoring, detection, and to facilitate the resolution of Problems.

   7.3. The ability to electronically link or associate Problems with records associated with related Incidents, Changes, Releases, and Configuration Items or components.

   7.4. A Known Error Database / Knowledge Database, used to capture, store, and retrieve information and solutions. This knowledge database will enable the sharing of the following:

      7.4.1. Policies and procedures for resolving or circumventing errors.

      7.4.2. Best practices for resolving or circumventing errors.

      7.4.3. Methods to Resolve Problems among DCS Service Provider personnel, Third Party Vendors, and Authorized Users.

      7.4.4. References for Configuration Items for Resolving or circumventing errors.

      7.4.5. Contain a taxonomy approved by DIR as collecting useful information.

   7.5. The Known Error Database / Knowledge Database which will record at a minimum the following information for each Problem / Known Error record:

7.5.1. Details of the Problem / Known Error fault.

7.5.2. Details of the symptoms recognized associated with the Problem / Known Error.

7.5.3. Details of workarounds and/or resolutions that were or can be used to address the Problem / Known Error in order to restore service and / or deal with the Problem / Known Error or any associated Incidents in the future.

7.5.4. Information regarding the business case / cost benefit analysis that was performed associated with the Problem / Known Error.

7.5.5. The identification of each configuration item / component that is affected by the Problem / Known Error.

7.5.6. The unique identifier for each Problem / Known Error record.

7.5.7. The category and priority of each Problem / Known Error record.

7.5.8. Status of the Problem / Known Error record.

7.5.9. Date / time stamps for when the Problem / Known Error record was created and date/ time stamps associated with any milestone achievement (e.g. diagnosis, solution identification, RFC submittal, resolution, etc.).

7.6. The ability to track and associate Problems and Known Errors with the Incidents that have occurred.

7.7. Provide for designation of Problems as opened with a known Resolution which will not be implemented at the discretion of DIR or DIR Customer due to unacceptable customer impacts (e.g. impractical Application changes, cost).

7.8. Securely segregate DIR and DIR Customer data so that it can be accessed only by those authorized to comply with Government security requirements and in accordance with DIR policy.

7.9. Provide for the tracking and reporting of RCA activities (e.g. which Problems have RCA underway, what RCAs have been reported, what RCAs have been requested, what RCAs require additional DIR or DIR Customer response).

7.10. Provide for logging all modifications to Problem Records, to provide full tracking, audit trail and change control at the named-user level.

8. Regularly update the Problem Management System (including the Known Error Database / Knowledge Database) with Service Provider and other designated Third Party Vendor solutions and best practices as they are developed, including updates based on “lessons learned” and experience with similar technologies and problems for other customers.

A.1.3.5 Communication and Notification

Service Provider’s responsibilities include:

1. Maintain accurate communications within designated timeframes and provide status reports through the Service Desk to DIR and DIR Customers and, as necessary, to other Service Component Provider(s) from the time a Problem is identified through Resolution.
2. Post-resolution, provide follow-up communications and status reporting as necessary.
3. Track and report any backlog of unresolved Problems on at least a monthly basis to the Problem Manager, or more frequently as requested by DIR.

A.1.3.6 Problem Management Reporting

Service Provider's responsibilities include:

1. Provide regular (weekly) and ad hoc electronic reports on an enterprise level, as well as by agency to the DIR Customer, on Problems including:
    - 1.1. Statistics on total numbers of Problems.
    - 1.2. Escalations and responsible entities.
    - 1.3. Outstanding Problems.
    - 1.4. Resolution time.
    - 1.5. Chronic outages.
    - 1.6. Performance.
    - 1.7. Problem trend analysis.
2. Provide a monthly report(s) to DIR and DIR Customers, in a format approved by DIR, that include at a minimum:
    - 2.1. The percentage and number of Problems in total and grouped by category, priority, severity, status, DIR Customer, system/component, region, classification or other criteria as appropriate.
    - 2.2. Information regarding Major Problem Reviews, including all details set out above.
    - 2.3. Information regarding Problem analyses and RCAs conducted in the previous period.
    - 2.4. Problem trend analysis findings.
    - 2.5. Information regarding new Known Error records and/or workarounds added to the Known Error Database / Knowledge Database (including number, category, priority, etc.).
    - 2.6. Details on the use and utility of the Known Error Database / Knowledge Database.
    - 2.7. Details regarding open Problem / Known Error, including identification number, description, status, date/time of record open, status description, etc.
    - 2.8. Results of reviews of Incidents to identify recurring Incidents and associated Problems.
    - 2.9. Tracking information as to escalations, contacts, follow-ups and commitments.
    - 2.10. Tracking information as to requests from DIR and DIR Customers' to initiate Problem Management.
    - 2.11. Any issues relating to the Problem Management process, such as any information that may improve or facilitate a better Problem Management process, including decisions to be made by DIR and Service Provider.
    - 2.12. Trend analysis of Problems reported during the thirteen (13) most recent months.

3. Provide a quarterly report(s) on the areas for improvement and on-going activities to correct Problem trending and prevent future Problems and Incidents, in a format agreed to by DIR.

A.1.4 Change Management

Change Management comprises an end-to-end solution that minimizes risk, cost and business disruption, while protecting the computing and the delivery of related Services. All changes to Configuration Items must be carried out in a planned and authorized manner. This includes identifying the specific Configuration Items and IT Services affected by the Change, planning the Change, communicating the Change, deploying the Change, testing the Change, and having a back-out plan should the Change result in a disruption of the Service. This also includes tracking and oversight for all Changes.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider personnel and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Change Management.
3. Validate that the Change Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider's Change Management process with the Change Management processes of DIR and other Service Component Provider(s), as well as authorized Third Party Vendor(s)' Change Management processes, with and where the processes interact.
5. Communicate and coordinate Change Management processes within Service Provider's own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).
   5.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Change Management processes.
6. Facilitate and lead in the definition and documentation of Change Management Policies, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Change Management processes.
   6.1. Continually verify the effective compliance with the Change Management Policies by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.
7. Cooperate with the Service Desk and Third Party Vendor(s) for Changes across all Applications, system components, and parties.
8. Coordinate Change Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.
9. Conduct regularly scheduled Change Management meetings at the enterprise and agency level (e.g. separate meetings for each agency each week).

9.1. Document and publish Change Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.

10. Establish the operation and composition of each Change Advisory Board and Emergency Change Advisory Board for DIR and DIR Customers, including membership, practices, tools (e.g. action lists, electronic meeting facilities, recording of approvals, etc.), agendas, cadence, etc; such Boards are outlined in the **Exhibit 6**.

11. Verify that all RFC are done through the appropriate form, meet the appropriate criteria, and follow the approved process.

12. Provide a standard RFC form that will be used to request Changes and that will remain in use throughout the life of the change until formal closure as called for by the Change Management Process.

12.1. Reject or return to the Requestor those RFCs which do not meet the criteria.

13. Summarize the Changes made and attempted each week, and report the information to DIR and DIR Customers on a weekly basis.

14. Capture all DIR Customer Change data centrally, and make it available to DIR, DIR Customer and Authorized Users.

15. Establish a single focal point for changes in order to minimize the probability of conflicting changes and potential disruption to the production environments.

16. The definition of change windows and black-out periods, including the enforcement and authorization for exceptions.

17. Conduct Post Implementation Reviews (PIR) on Changes as requested by DIR.

18. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Change Management Process.

19. Provide a change categorization schema that will be used to categorize all changes, and approved by DIR.

20. Provide a change prioritization schema that will be used to prioritize changes, and is approved by DIR.

21. Coordinate the establishment and routine update of maintenance periods for Service Provider and other Service Component Provider(s), which support both the regular and normal maintenance of the Infrastructure and Services while protecting DIR and DIR Customers from undo risk and unplanned outages.

22. Routinely maintain a current Projected Service Outage document (in conjunction with the Availability Management process) which defines and sets out details regarding scheduled service outages, for both regularly scheduled maintenance outages and other scheduled outages, and provide the document and report on Projected Service Outages to DIR and DIR Customers as required.

23. Report to DIR and DIR Customer on change activity in the Enterprise that presents undo risk and propose actions to address.

A.1.4.1 General Change Management

Service Provider’s responsibilities include:

1. Verify that the effective execution of the Change Management Process, as well as an appropriate review of planned changes, takes place with due consideration of the business and technology risk of planned changes, taking into consideration all defined criteria (such as complexity of change, the skill level of the individual(s) executing the change, the planned change execution timeframe, the change slot timeframe, the back-out timeframe, pre-change technical deployment planning, communication planning, post-change validation planning, and the relevant business processing criticality).
2. With proper authorization, stop any planned changes that, in the professional view of the person(s) performing the Services, would compromise the continuation of Services to DIR and DIR Customers, and act as the gatekeeper to production, unless expressly overridden by the DIR’s Operations Manager in accordance with the approved Change Management escalation process.
    2.1. Assume responsibility for escalating and ensuring parties responsible for resolution are properly engaged for any issues arising from the decision to stop a planned change.
3. Monitor change closure status for appropriate success/failure classification. Manage and conduct the review of any change failures, and provide a strong interlock between change and Incident Management and Problem Management processes so that post-change issues can be linked to the change activity where relevant. Continuously work with Service Provider staff to understand success/failure criteria and integration requirement with Incident and Problem Management.
4. Manage to Resolution any deviation from effective Change Management Process, ensuring the purposeful review and closure of failed changes.
5. Do not make changes that (i) may adversely affect the function or performance of, or decrease the resource efficiency of the Services, (ii) increase DIR's and DIR Customers’ costs or fees, or (iii) impact the way in which DIR and DIR Customers conduct their business or operations, without obtaining prior DIR and DIR Customer approval via the Change Management process.
6. Provide a procedure for requesting changes in the process used for making Service Requests.
7. Provide a means for changes to be requested from all relevant stakeholders, including DIR, DIR Customers, Service Provider, and Third Party Vendors.
8. Provide a complete and accurate RFC form to request Changes, including all details per process guidelines on Change requests.
9. Raise and record Changes using the standard RFC form.
10. Review the RFC to ensure the RFC meets the following criteria:
    10.1. The RFC was correctly and fully completed.
    10.2. The RFC comes from an authorized requestor.
    10.3. The RFC does not request a change that would on its face violate prohibiting policies.

10.4. The RFC does not duplicate an existing request.

11. Assess, document, and communicate all proposed Changes in terms of the following at a minimum:

    11.1. Business impact.

    11.2. Technical feasibility.

    11.3. Business benefit and/or value.

    11.4. Risk.

    11.5. Intended results and outcomes of the change.

    11.6. Resources required to plan, execute and validate the change, which includes insuring cross-technical teams are appropriately engaged throughout the change-lifecycle.

    11.7. Relationship of the requested change to other changes (e.g., identify conflicts or opportunities to package changes together).

    11.8. Schedule of the change.

12. Provide and maintain compliance with DIR policies.

13. Confirm business justification and obtain approval.

14. Coordinate the change build, test and implementation activities.

15. Perform Changes in DIR Customers’ IT environments pertaining to the Services, including Changes to individual components and coordination of Changes across all components.

16. Verify Changes are in accordance with Change Management procedures approved by DIR.

17. Provide and update a Projected Service Outage document which defines and sets out details regarding project service outages – both scheduled maintenance outages and ad hoc outages.

18. Monitor and report progress, issues and status related to Change implementation to all relevant parties.

19. Develop, utilize, manage and continually improve an inventory of defined and documented Change Models, for repeatable Change activity and process, that incorporates the following elements:

    19.1. Sequences of tasks, actions or steps to execute the Change and resolve the Incident.

    19.2. Identification of required dependencies, data sources, etc. that must be considered in executing the Change Model.

    19.3. Definition of responsibilities and roles to execute the Change Model.

    19.4. Timescales, milestones and thresholds for executing the Change Model.

    19.5. Anticipated escalation points and escalation procedures associated with the Change Model.

19.6. Tasks, activities, methods, tools, systems, etc. to ensure that detailed audit information be recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DIR Customer data.

20. Provide a documented list of Standard Changes in appropriate DIR and DIR Customer documents which are pre-approved changes for a specific, low-risk change that has a defined Change Model and a defined set of processes and procedures.

21. Review all changes in terms of the following:

21.1. Success or failure (based on the established criteria for change success or failure established in the policies and procedures for the Change Management process or the Change).

21.2. Operational soundness of the services offered to DIR and DIR Customers and the technical systems and components that support them following the change.

21.3. Proper completion of all required change documentation (based on the established policies and procedures for the Change Management process).

22. Close all Changes following a review of each change with other Service Component Provider(s) and DIR Customer.

23. Deploy workflow-based tools to automate the process of recording, assessing, scheduling, describing, authorizing, tracking, and reporting on Changes.

24. Collect data on every Change attempted, including:

24.1. The reason for Change.

24.2. Detailed description of Change.

24.3. Whether the Change was successful from the perspective of the Authorized Users of the system.

25. Provide an audit trail of any and all Changes in order to determine the Change made and the authorization to make the Change.

A.1.4.2 Change Management System

Service Provider’s responsibilities include:

1. Develop and implement a standardized method and procedure for the efficient and effective handling of all Changes (an overall Change Management process), including the Change Advisory Boards (CAB) to manage Changes to the Services, subject to approval from DIR, in a way that minimizes risk exposure and maximizes availability of the Services.

2. Deploy tools and processes to automate the recording, assessing, scheduling, documenting, tracking, and reporting on Changes to the environment.

3. Integrate the Change Management System with Service Provider’s other Service Management processes and systems, including Incident Management, Problem Management, Asset/Inventory Management, Configuration Management, Release Management and IT Service Continuity Management.

3.1. Integrate Change Management tools to the CMS / CMDB.

4. Provide access to the Change Management System, including associated tools, to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors; which access shall include all appropriate and required licenses and/or interfaces.
5. Enable data exchange between the Change Management Systems and the change management systems of other Service Component Provider(s), DIR Customers and designated Third Party Vendors, as directed by DIR.
6. Limit access to the Change Management System and tools to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.
7. Provide for logging all modifications to Change Records, to provide full tracking, audit trail and change control at the named-user level.
8. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the Change Management System, tools and processes.
9. Provide a standard RFC form that will be used to request Changes and that will remain in use throughout the life of the change until formal closure as called for by the Change Management Process, and that will include the following information at a minimum:
   - 9.1. A unique identifier for the Change.
   - 9.2. A description of the Change.
   - 9.3. The purpose and justification for the Change (including information about the impact of not implementing the Change).
   - 9.4. A list of Service(s), DIR Customer Applications, Authorized User(s), and Third Party Vendor(s) potentially affected by the Change.
   - 9.5. A list of items to be changed and/or affected by the Change.
   - 9.6. The category of the Change.
   - 9.7. The priority of the Change.
   - 9.8. Details of the assessment conducted for the Change.
   - 9.9. Change authority / approver.
   - 9.10. Date / time of change approval.
   - 9.11. Decisions and recommendations accompanying the approval.
   - 9.12. The proposed schedule, including implementation date(s) and approximate time(s) for determination of any existing conflict with business events.
   - 9.13. The proposed implementation plans / procedures.
   - 9.14. Identification of the Change Builders, Change Testers and Change Implementers.
   - 9.15. Details of the Change implementation – including date / time and details of activities executed.
   - 9.16. Change review details, including method of review, review findings, etc.
   - 9.17. Details and links with other tickets, records and documentation related to incidents, problems, changes, releases, etc.

9.18. Closure details, including date / time and who closed the record.

9.19. Detailed description of the communication plan associated with the Change.

A.1.4.3 Process and Procedures

Service Provider’s responsibilities include:

1. Follow established Change Management Process and Policies, which include for the following:

1.1. Handling unauthorized change.

1.2. Standard change documentation.

1.3. Communicate the Change Management process with appropriate stakeholders and provide appropriate training.

1.4. Prioritization of change.

1.5. Categorization of change.

1.6. Classification of risk associated with change.

1.7. Definition and handling of Emergency Changes, including requirements for documentation, approval, planning, review, etc.

1.8. Assessment of Changes (methods, tools, etc. based on category and priority and using standard tools such as a Change Risk and Prioritization Matrix).

1.9. Creation and use of Change Models for repetitive Changes to improve the efficiency and effectiveness of the Change process.

1.10. Approval of change – including levels of authorization, methods of approval documentation, etc.

1.11. Establishing accountability and responsibilities for changes through the service lifecycle.

1.12. Provide for segregation of duty controls.

1.13. Preventing people who are not authorized to make a change from having access to the production environment.

1.14. Integration with other Service Management processes to establish traceability of change, detect unauthorized change and identify change related incidents, and to support the proper execution of the other Service Management processes.

1.15. Criteria for assessment / evaluation of all changes.

1.16. Criteria for reviewing changes, including Post Implementation Reviews, and including policies and procedures for reviews to be conducted after a pre-determined period of time to establish that:

1.16.1. The change has had the desired effect and met its objectives.

1.16.2. Users, customers and other stakeholders are content with the results, or to identify any shortcomings.

1.16.3. There are no unexpected or undesirable side-effects to functionality, service levels, warranties, availability, capacity, security, performance, continuity readiness and costs.

1.16.4. The release and deployment plan worked correctly.

1.16.5. The change was implemented on time and to cost.

1.16.6. The remediation plan functioned correctly, if needed.

1.17. Escalation and handling of failed changes.

1.18. Grouping / packaging changes.

1.19. Performance measures for the process, including measures for efficiency and effectiveness.

2. Document the Change Management process and procedures in accordance with the requirements in **Attachment 6-B**.

3. Maintain clear ownership for individual Changes throughout the process.

4. Identify when change management procedures or policies have not been followed and coordinate with associated and appropriate parties to establish plans for correcting.

5. Manage the Change Process such that proposed Changes are submitted in advance to the Change Advisory Board.

6. At a minimum, each submitted proposed Change will include:

6.1. A unique identifier for the Change.

6.2. A description of the Change.

6.3. The purpose and justification for the Change (including information about the impact of not implementing the Change).

6.4. A list of Service(s), Authorized User(s), and Third Party Vendor(s) potentially affected by the Change.

6.5. A list of items to be changed and/or affected by the Change.

6.6. The category of the Change.

6.7. The priority of the Change.

6.8. Details of the assessment conducted for the Change.

6.9. Change authority / approver.

6.10. Date / time of change approval.

6.11. Decisions and recommendations accompanying the approval.

6.12. The proposed schedule, including implementation date(s) and approximate time(s) for determination of any existing conflict with business events.

6.13. The proposed implementation plans / procedures.

6.14. Identification of the Change Builders, Change Testers and Change Implementers.

6.15. A rating of the potential risk, business impact, and/or complexity of the Change.

7. Where a proposed Change represents a potentially high risk or high impact to DIR Customers’ operations or business, or at the request of DIR Customer, Service Provider will also include a comprehensive end-to-end test plan (including clear Change acceptance criteria), notification and escalation lists, and work-around plans.

7.1. In terms of change planning standards, the concept of comprehensiveness should apply consistently across risk levels and whether the change planning is for an agency change or an enterprise change; a comprehensive plan should include at least the following:

7.1.1. A full description of the change including the purpose of the change.

7.1.2. Pre-Installation planning (where possible includes demonstrating testing in non-production environments).

7.1.3. Communication planning (Includes communications throughout the life cycle of the change).

7.1.4. Installation planning.

7.1.5. Post-Installation planning (includes testing and validation).

7.1.6. Impact analysis (impact of performing and not performing the change).

7.1.7. Complete planning with cross-Service Component entities.

7.1.8. Include a comprehensive contingency plan, including a back-out plan and procedures (with specific criteria as to when to initiate the execution of the back-out plan).

8. Verify compliance with DIR policies.

9. Categorize all changes.

10. Prioritize all changes.

11. Review proposed Changes and schedules with DIR Customers, and obtain all necessary approvals for proposed Changes.

12. Coordinate with DIR, DIR Customers, all affected Third Parties and designated representatives at Sites potentially affected by a Change in order to minimize disruption of normal business processes.

13. Control system Changes and activities required by moves, upgrades, replacements, migrations, and so forth.

14. Include rollout, testing, and roll-back / remediation plans for every RFC as part of the information used for change approval.

15. Provide a regularly updated and reported Change Schedule that includes details of all scheduled changes.

16. Ensure that the Configuration Management System / Database is updated throughout the process.

17. Provide information to DIR, DIR Customers in accordance with the Change Management process on the outcome of any RFC and the updated status after each Change is implemented.

18. Update all operational and other documentation affected by the Change.

19. Report the status of scheduled Changes, including maintaining a comprehensive list of projects and dates.

20. Collect data on every Change attempted, which includes the following:

20.1. Include the cause of any Incidents, measures taken to prevent recurrence, and whether the Change was successful from the perspective of the Authorized User or Third Party affected by the Change.

20.2. Summarize and report this data to DIR on a weekly basis.

21. Provide an audit trail of any and all Changes to all environments, which should include a record of the Change made and the authorization to make the Change.

22. Conduct Post Implementation Reviews (PIR) on Changes, if requested by DIR or DIR Customer.

23. Provide DIR with the ability to pre-approve certain types of routine operational Changes (Standard Changes). Such approvals shall be documented in the Service Management Manual, described in **Attachment 6-B**.

A.1.4.4 Maintenance Periods

Service Provider's responsibilities include:

1. Establish and document periods for maintenance in the Service Management Manual, understanding that there will be at least 29 separate maintenance periods initially for individual DIR Customers in addition to maintenance periods established for the Consolidated Data Centers.

   1.1. Establish periods for routine and regular maintenance for all Equipment and Services under Service Provider management.

   1.2. Establish specific periods for Enterprise maintenance effecting multiple organizations (e.g. shared infrastructure).

   1.3. Establish processes for scheduling and getting approval of other maintenance (e.g. urgent but non-emergency).

   1.4. Establish processes for coordinating and planning maintenance periods with other Service Component Provider(s) and Third Party Vendors as appropriate.

   1.5. Establish communications plans to support maintenance and appropriately inform other Service Component Provider(s), DIR, DIR Customers and Third Party Vendors.

2. Regularly communicate and re-communicate the established maintenance periods with DIR and DIR Customers, and as necessary communicate any time maintenance periods are revised.

3. Perform maintenance during regular Maintenance Periods as defined in the Service Management Manual, or as scheduled in advance with the approval of DIR or DIR Customers.

4. Validate that systems will be unavailable during maintenance windows only to the extent necessary for systems maintenance purposes.

5. Provide at appropriate notice to DIR and DIR Customers of the maintenance to be performed during scheduled maintenance windows, based on the categorized risk of the Change and as specified in the Service Management Manual.

6. Change scheduled maintenance windows at DIR's or DIR Customer's request and upon reasonable notice.

7. Schedule Outages for maintenance, expansions, and modifications during hours that meet DIR's and DIR Customers' business needs.
8. Stagger maintenance as appropriate to accomplish all work across all DIR Customers within the establish time-frames and based on the categorized risk of the Change.
9. Allow DIR and DIR Customer, at any time at its discretion, to specify "freeze" periods during which Service Provider and Third Party Vendors will not make any Changes.
10. If there is a need for emergency systems maintenance, provide other Service Component Provider(s), DIR, DIR Customers and Third Party Vendors with as much notice as reasonably practicable, and perform such maintenance so as to minimize interference with the business and operational needs of DIR and Customers.
11. Ensure that Changes to the environment are fully tested and any faults are Resolved, including and as practical, prior testing for inter-operability.

A.1.4.5 Change Management Reporting

Service Provider's responsibilities include:

1. Create and maintain a Change Schedule of upcoming Releases and Changes as part of the Change Management process.
2. Provide monthly reports in a format agreed with DIR as described in **Exhibit 13** and includes at a minimum a breakdown of metrics by type, category, priority, effected service or system, and success/failure.
3. Provide a weekly report in a format agreed with DIR that, at a minimum, includes:
   - 3.1. The status of all Changes active at the beginning of the week and all Changes raised during the week.
   - 3.2. The Changes to be implemented the following week.
   - 3.3. The Changes submitted for approval.
4. Schedule, participate and lead regularly scheduled Change Advisory Board meetings with DIR, DIR Customers and Third Party Vendor(s) as described in **Exhibit 6**.
5. Review proposed Changes and schedules through a formal walk-through process with DIR, DIR Customers and Third Party Vendor(s), and obtain all necessary approvals for proposed Changes.
6. Provide statistical reporting on change activity to DIR as requested.

A.1.5 Configuration Management

Configuration Management will provide a logical model of the IT infrastructure by identifying, controlling, maintaining, and verifying information related to all Configuration Items that support the Services offered to DIR and DIR's Customers.

Configuration Management will include the implementation of a system (the Configuration Management System) which incorporates information from multiple databases (Configuration Management Databases – CMDBs) that contains details of the components or configuration items (CIs) that are used in the provision, support and management of its IT services. This is more than just an "asset register," since it will contain information that relates to the maintenance, movement, and problems experienced with the CI, and their relationships. The CMS or the DIR records that reside within Service Provider-provided CMS will be DIR Data.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Configuration Management.
3. Validate that the Configuration Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider’s Configuration Management process with the Configuration Management processes of DIR and other Service Component Provider(s), as well as authorized Third Party Vendor(s)’ Configuration Management processes, with and where the processes interact; including providing Configuration data electronically to DIR’s CMS / CMDB.
5. Integrate Service Provider’s Configuration Management process with the other Service Management processes, including Incident Management, Problem Management, Change Management, and Release Management.
6. Coordinate Configuration Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customers.
7. Communicate and coordinate the Configuration Management processes and policies within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).
    - 7.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Configuration Management Process.
8. Define Configuration Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Configuration Management process.
    - 8.1. Continually verify the effective compliance with the Configuration Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.
9. Create and maintain a Configuration Management Plan, including a Configuration Management Validation Plan that is agreed to by DIR.
    - 9.1. Continually verify the effective execution of the Configuration Management Plan, including the Configuration Management Validation Plan, by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

A.1.5.1 General Configuration Management

Service Provider’s responsibilities include:

1. Conform operations to policies and procedures that set the objectives, scope and principles that will ensure the success of the Configuration Management process, including compliance with policies and procedures for the following:

   1.1. Ensuring that Configuration Management operations costs and resources are commensurate with the potential risks to the Services.

   1.2. The need to deliver state governance requirements (e.g. software asset management, audits).

   1.3. The need to deliver the capability, resources and service warranties as defined by the service level agreements and contracts.

   1.4. Defining how the taxonomy, classes and types of assets and configuration items are to be selected, grouped, classified and defined by appropriate characteristics (e.g. warranties for a service, to ensure that they are manageable and traceable throughout their lifecycle).

   1.5. Defining the approach and schemas for identification, uniquely naming and labeling all the assets or service components of interest across the service lifecycle and the relationships between them.

   1.6. Performing the roles and responsibilities of the owner or custodian for configuration item type at each stage of its lifecycle.

   1.7. Provide and maintain adequate asset and configuration information for internal and external stakeholders.

   1.8. Maintain the level of control and requirements for traceability and audit compliance.

   1.9. The application of continual improvement methods to optimize the service levels, assets and configurations.

   1.10. Provision of accurate asset and configuration information for other business and Service Management processes.

   1.11. Migration of Service Provider infrastructure information to a common asset and CMS architecture.

   1.12. Provide automation to reduce errors and costs.

2. Use a Configuration Management process to:

   2.1. Identify CIs, such as Operations Documents, Equipment, Software and Applications used to provide the Services, including the following:

      2.1.1. Define and document criteria for selecting configuration items and the components that compose them according to the taxonomies, policies and procedures agreed to in the Service Management Manual.

      2.1.2. Select the configuration items and the components that compose them based on documented criteria.

      2.1.3. Assign unique identifiers to configuration items.

      2.1.4. Specify the relevant attributes of each configuration item.

2.1.5. Specify when each configuration item is placed under Configuration Management, including relationships to any existing configuration items and assuring that all changes to CMDB to include an audit trail.

2.1.6. Identify the owner responsible for each configuration item.

2.1.7. Specify relationships, affinities and associations to other configuration items (e.g. relationship between Applications, cross Application dependency).

2.2. Maintain accurate configuration data for the Configuration Items, including Operations Documents, Equipment, Software and Applications used to provide the Services.

2.3. Verify that only authorized and identifiable Configuration Items, including Operations Documents, Equipment, Software and Applications are accepted and recorded throughout their lifecycle.

2.4. Record, maintain and reproduce the configuration status of the Configuration Items, including Operations Documents, Equipment, Software and Applications, at any point in time throughout its life cycle.

2.5. Conduct reviews and validation to verify the physical existence of Configuration Items, including Operations Documents, Equipment, Software, and Applications, and to check that they are correctly recorded in the CMS / CMDB.

2.6. Produce and maintain current Equipment, Software, and Application architecture and design documentation for issue to DIR and DIR Customers upon request.

3. Conform Service Provider operations to Configuration Management Policies and Procedures that at a minimum articulate the following:

3.1. Define the roles and responsibilities of the owner or custodian for configuration item type at each stage of its lifecycle.

3.2. Define adequate asset and configuration information for internal and external stakeholders.

3.3. Define the level of control and requirements for traceability and audit compliance.

3.4. Define taxonomies for criteria used to select CIs and their components.

3.5. Define schema and guidelines for assigning unique identifiers to configuration items.

3.6. Provide effective categorization and classification structures to support the proper documentation and maintenance of Configuration Items, and Configuration Models.

4. Follow the established categorization and classification structures to support the proper documentation and maintenance of Configuration Items and Configuration Models.

5. Use the Configuration management process to identify, control, maintain, and verify the CIs approved by DIR as comprising the Equipment, Software, and Applications to provide the Services.

6. Provide Configuration Models as a reliable and complete model of the services, assets and the infrastructure by recording the relationships between configuration items (e.g. relationships, affinities and associations to other Applications, services and equipment), in order to provide other processes with the information needed

7. Verify that all CIs for the Equipment, Software, and Applications are incorporated into the CMS / CMDB.

8. For each CI, use at least the attributes specified by the Configuration Management policies and procedures.

9. Ensure that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and ownership so that no CI will be added, modified, replaced or removed without appropriate controlling documentation and an appropriate procedure being followed.

10. Validate that any change to any CI record in the CMDB is the result of an approved Request for Change.

    10.1. Validate the integrity and currency of the CMDB by continually validating the content of the CMDB against the CIs that have been executed against the Services.

    10.2. Take corrective actions through the Incident Management process.

11. Perform logical validation of all Equipment, Software, and Applications used to provide the Services in accordance with the Configuration Management Validation Plan, in order to:

    11.1. Verify the existence of CIs recorded in the CMS / CMDB.

    11.2. Check the accuracy and completeness of the records in the CMS / CMDB.

    11.3. Identify any CIs not recorded in the CMS / CMDB.

    11.4. Formally record exceptions discovered in the validation effort.

12. Take corrective action if a physical validation identifies any deficiency in the accuracy or completeness of the records in the CMS / CMDB.

13. Provide required information to secure libraries (both physical and electronic) in which the definitive authorized versions of all media CIs are stored and protected and which are used for controlling and releasing components throughout the service lifecycle.

14. Provide Configuration Baselines which detail the configuration of the service, product or infrastructure that has been formally reviewed and agreed on, and that captures the structure, contents and details of the configuration as a set of configuration items that are related to each other.

15. Establish a baseline of CIs and services before a release into a Development, Test, or Production environment.

16. Provide snapshots of the current physical configuration of a service, system or set of configuration items upon request and for use in problem analysis, incident restoration, security management, etc.

17. Verify release and configuration documentation before Changes are made to the live environment.

18. Maintain a secure audit trail of all CMS / CMDB transactions.

19. Maintain a Configuration Management Plan, including a Configuration Management Validation Plan, that is agreed to by DIR, that articulates the following:

19.1. The scope of the Configuration Management process in terms of the Services supported, the systems, environments, Operations Documents, Equipment, Software and Applications etc.

19.2. The policies and procedures that ensure the success of the Configuration Management process.

19.3. The activities of the Configuration Management process.

19.4. The roles and responsibilities of the Configuration Management process.

19.5. The systems and tool that support the Configuration Management process, including the CMS / CMDB, discovery tools, validation and verification tools, storage libraries, etc.

19.6. Integration with and relationships with other Service Management processes.

19.7. How the success of the process will be monitored, measured and reported.

19.8. Maintain a Configuration Management Validation Plan, that is agreed to by DIR that articulates the following:

19.8.1. Continual assurance of an accurate CMS / CMDB.

19.8.2. Monthly random sampling of CMDB for accuracy of logical data.

19.8.3. An annual inventory of Service Provider assets and Equipment under management and required for the delivery of Services.

19.8.4. An annual inventory of all logical information of the CMDB.

19.8.5. Perform all validation and reconciliation activities associated with inventory, including updates to the CMDB.

A.1.5.2 Configuration Management System

Service Provider’s responsibilities include:

1. Provide and maintain a CMS / CMDB that will serve as the single source of information regarding all Configuration Items for Service Provider Services, other Service Component Provider(s) Services, and designated Third Party Vendors.

1.1. Provide access to the CMS / CMDB to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors, which access shall include all appropriate and required licenses and/or interfaces.

2. Ensure that all Configuration data related to the Services resides in the CMS / CMDB.

3. Integrate the CMS / CMDB with other systems for Service Management, including Incident Management, Problem Management, Change Management, and Release Management.

4. Integrate the CMS / CMDB with the Configuration Management Systems of other Service Component Provider(s) and designated Third Party Vendors.

4.1. Integrate the CMDB with the Configuration Management Databases of other Service Component Provider(s), and designated Third Party Vendor(s), as directed by DIR.

4.2. Enable interfaces to integrate with the CMS / CMDB of other Service Component Provider(s), DIR, DIR Customers and authorized Third Party Vendors, as directed by DIR.

5. Limit access to the CMS / CMDB to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

6. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the CMS / CMDB.

7. Grant DIR and DIR Customers access to the database(s) of the CMS / CMDB, and allow DIR to monitor and view on an ongoing basis.

8. The CMS / CMDB shall at a minimum support the following:

    8.1. Maintain the relationships between all service components and any related incidents, problems, known errors, change and release documentation.

    8.2. Provide a customizable set of views for different stakeholders through the service lifecycle.

    8.3. Consolidate data from several physical CMDBs as necessary, which together constitute a federated CMS.

    8.4. Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to load and update the CMS / CMDB.

    8.5. Mapping of logical information to physical assets (e.g. Applications, software, DR RTO/RPO, Billing Field, virtual server instance associations with physical hosts)

9. Maintain the CMS / CMDB to meet performance standards, to maximize efficiency, and to minimize outages, as necessary.

    9.1. Designate performance standards for the CMS / CMDB in the Service Management Manual.

10. Maintain, update, and implement the CMS / CMDB archive processes and procedures needed to recover from an outage or corruption within designated timeframes in order to meet DIR and DIR Customers’ business requirements.

11. Provide CMS / CMDB physical database management support, including providing backups and restores of data within designated timeframes.

12. Install, maintain, and support CMS / CMDB related database Software products.

13. Test and implement CMS / CMDB database environment changes, as approved by DIR.

14. Proactively provide capacity planning for the CMS / CMDB to prevent situations caused by lack of capacity (i.e. dataset or table space capacity events, full log files, etc.).

15. Correct situations caused by lack of CMS / CMDB capacity within designated timeframes (i.e. dataset or table space capacity events, full log files, etc.).

A.1.5.3 Configuration Management Reporting

Service Provider’s responsibilities include:

1. Provide a monthly report on configuration Changes made to the infrastructure, Equipment, and Software.
2. Provide a monthly report in a format agreed by DIR, to include:
    - 2.1. Number and classification of configuration Changes made.
    - 2.2. Trend analysis of the configuration Changes made during the thirteen (13) most recent months.
3. Provide a report within ten (10) Business Days of completion of a validation effort, as part of the Configuration Management Validation Plan, covering at a minimum:
    - 3.1. Number of differences between the records and validation effort findings.
    - 3.2. Number of occasions on which a configuration was found to be unauthorized.
    - 3.3. Recommended corrective actions to Resolve any process deficiencies or failures identified.
    - 3.4. Number of occasions on which a recorded CI could not be located.
    - 3.5. Statistical information about the structure and composition of the Equipment and Software.
4. Provide monthly exception reports which articulate the following:
    - 4.1. Number of instances where configuration information in the CMS / CMDB was discovered to be incorrect (e.g. when being used to execute support and delivery activities, and activities of other processes).
    - 4.2. Details of the Exception Reports created as a result of the configuration validation.
    - 4.3. Details regarding instances in which configuration policies and procedures have been violated.
5. Provide reports regarding Configuration Items and configurations as requested by DIR and DIR Customers.
6. Provide Portal access to the CMS / CMDB for authorized DIR and DIR Customer ad hoc reporting, including access to the data dictionary and user documentation.

A.1.6 Release Management

The purpose of Release Management is to build, test and deliver the capability to provide the specified Services and that will accomplish the stakeholders’ requirements and deliver the intended objectives, and to establish effective use, delivery and support of the Service and its underpinning technologies and processes.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Develop and establish a Release and distribution process so that each Change to Services is controlled, tested, traceable, authorized, and implemented in a structured manner.

3. Support information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer to improve end-to-end Release Management.
4. Validate that the Release Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
5. Integrate Service Provider's Release Management process with the Release Management processes of DIR Customers and other Service Component Provider(s).
6. Integrate Service Provider's Release Management process with the other Service Management processes, including Incident Management, Problem Management, Change Management, and Configuration Management.
7. Support Release Management activities across all Service Provider and Service Component Provider(s) functions that provide Services to DIR and DIR Customers.
8. Communicate and coordinate the Release Management processes, policies and procedures within Service Provider's own organization, other Service Component Provider(s), DIR, and DIR Customers.
   - 8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, and DIR Customers on the Release Management Process.
9. Define Release Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Release Management Process.
   - 9.1. Routinely verify the effective compliance with the Release Management Policies and Procedures by Service Provider and other Service Component Provider(s).
10. Cooperate and work with Service Component Provider(s) to maintain the Release Management Plan that is agreed to by DIR.
    - 10.1. Routinely verify the effective execution of the Release Management Plan, by Service Provider and other Service Component Provider(s).

A.1.6.1 General Release Management

Service Provider's responsibilities include:

1. Define and establish Release Management Policies and procedures which support the following:
   - 1.1. Coordinate with other Service Component Providers and DIR Customer to ensure the provision of requested support as needed for a successful deployment.
   - 1.2. Define agreed upon release and deployment plans, including the overall Release Management Plan and Release schedule, with DIR and DIR Customers.
   - 1.3. Ensure that each release package consists of a set of related assets and service components that are compatible with each other.
   - 1.4. Ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the CMS.

1.5. Ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate.

1.6. Ensure that organization and stakeholder change is managed during the release and deployment activities.

1.7. Record and manage deviations, risks, issues related to the new or changed service and take necessary corrective action.

1.8. Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities.

1.9. Ensure that skills and knowledge are transferred to operations and support staff to enable them to effectively and efficiently deliver, support and maintain the service according to required warranties and service levels.

1.10. The definition, identification and management of release units.

1.11. The definition, identification and use of release design options.

1.12. The identification, design and management of releases and release packages.

1.13. The identification, design and management of release models.

1.14. The planning, execution and management of testing methods, tools and procedures.

1.15. The use of pilots.

1.16. The definition of release success / failure criteria for each point in the Release lifecycle.

1.17. Establish measurement processes to record the success and failure of Releases, including recording Incidents related to Release activities in the period following a Release.

2. Perform tracking of the Release Management Plan and oversight of functions against the execution of the plan.

3. Participate in the formal review and close of Releases (e.g. post-mortem review), including the following:

3.1. Capturing experiences and feedback on customer, user and Service Provider satisfaction with the deployment, e.g. through feedback surveys.

3.2. Highlighting quality criteria that were not met.

3.3. Checking that any actions, necessary fixes and changes are complete.

3.4. Reviewing open changes and ensure that responsibility for open changes are agreed before handover.

3.5. Reviewing performance targets and achievements.

3.6. Ensure there are no capability, resource, capacity or performance issues at the end of the deployment.

3.7. Checking that any problems, known errors and workarounds are documented and accepted.

3.8. Recording and addressing risks.

3.9. Confirming that the service has been accepted from early life support into Service Operations.

A.1.6.2 Release Management Reporting

Service Provider's responsibilities include:

1. Provide a monthly Release report(s) in a format agreed with DIR as described in **Exhibit 13**, which report(s) will at a minimum include:

   1.1. Number of Releases grouped by category and status.

   1.2. Success rate of Releases, including number of successes, reversals, corrections, and those causing business disruptions.

   1.3. Number and percentage of incidents and problems that are caused by failed releases.

   1.4. Description of the cause of failed releases.

   1.5. Trend analysis of the Releases reported during the thirteen (13) most recent months.

   1.6. Planned Release schedule and progress reports against Projects.

2. Maintain a secure audit trail of all Releases.

3. Provide the reports and notices detailed in the Release Management process for each Release.

4. Provide reports on changes to Definitive Media Library, as required by DIR and DIR Customers. Report at a minimum should include:

   4.1. Owner of software / hardware asset.

   4.2. Source of change (e.g. Incident number, change request, service request, problem).

A.1.6.3 Pre-Production Testing

Service Provider's responsibilities include:

1. Perform integrated pre-production testing, for all Service Provider supported Software (e.g. ITSM, Chargeback, Portal).

A.1.7 Request Management and Fulfillment

Service Provider shall be responsible for the enabling and managing all requests for DCS related Services from DIR and DIR Customers from the initial request through fulfillment of such requests via Services from multiple sources, such as other Service Component Providers, Third Party Vendors, DIR or DIR Customers.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).

2. Facilitate and lead in the implementation and maintenance of Request Management and Fulfillment processes that are flexible and facilitate effective communication and coordination across all functional areas, with other Service Component Provider(s) DIR and DIR Customers.

3. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Request Management.

4. Integrate Service Provider’s Request Management process with the Request Management processes of DIR and other Service Component Provider(s), as well as authorized Third Party Vendor(s)’ Release Management processes, with and where the processes interact.

   4.1. Facilitate the automation or mechanization of Service Requests between Service Provider, other Service Component Provider(s) and other Third Party Vendor systems.

5. Integrate Service Provider’s Request Management process with the other Service Management processes, including Incident Management, Change Management, Configuration Management, Release Management and Program Management.

6. Validate that the Request Management processes provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.

7. Coordinate Request Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customers.

8. Establish on-going working relationship with the other Service Component Provider(s) DIR and DIR Customers for effective Request Governance and the overall effective execution of the Request Management processes across all DIR Service Provider(s), and in compliance with the Governance provisions of this agreement.

9. Designate end-to-end responsibility to a single Service Provider and ownership for each Service Request to a single Service Provider staff member, thus minimizing redundant contacts with the Authorized User.

10. Communicate and coordinate the Request Management processes and policies within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

    10.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Request Management Process.

11. Facilitate and lead in the definition and documentation of Request Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Request Management processes.

    11.1. Continually verify the effective compliance with the Request Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

12. Lead in developing and establishing Request for Solution processes and appropriate mechanisms for the fulfillment of complex requests, requiring design, price, solution and proposals; including appropriate communications to adequately set expectations and promote good customer service.

13. Lead in developing and establishing Request for Solution processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.

14. Provide criteria and establish processes for properly establishing the priority of Service Requests.

    14.1. Prioritize Service Requests from VIP or Executive Users or as authorized by DIR or DIR Customers.

15. Provide criteria and establish processes to support the proper procedure for requesting the expedited handling of Service Requests.

    15.1. Expedite the handling of Service Requests from VIP or Executive Users or as authorized by DIR or DIR Customers.

16. Provide criteria and establish processes for DIR, DIR Customers, and designated Third Party Vendor(s) to escalate Service Requests.

    16.1. Escalate a Service Request where the Service Request cannot be completed within the relevant Service Levels or agreed timeframe, in accordance with the relevant Service Management Manual.

17. Establish processes that properly route Service Requests across multiple Service Providers and organizations.

18. Retain overall responsibility and ownership of all Service Request until the Service Request is completed subject to DIR Authorized User approval.

19. Develop and establish guidelines for closing Service Requests that support only closing Requests after receiving confirmation from the affected Authorized User.

    19.1. Develop and establish guidelines for closure where Authorized Users confirmation has not been received.

A.1.7.1 General Request Management

Service Provider’s responsibilities include:

1. Manage the effective execution of Request Management to achieve its primary purpose to fulfill service requests within the agreed Service Levels and promote Customer and Authorized User satisfaction.

2. Provide for mechanisms to support ordering and billing to other Service Component Provider(s) and designated Third Party Vendors, for requests associated with the delivery of Services and where authorized by DIR or DIR Customers.

3. Ensure that detailed audit trail information be recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DIR Customer data.

4. End-to-end traceability must be provided even when transactions span across multiple Applications, systems components, or parties.

5. Provide effective Request Governance to ensure the following:

   5.1. Clearly define and document the type of Service Requests that will be handled within the Request Management process so that all parties are absolutely clear on the scope of Service Requests and the Request Management process.

   5.2. Establish and continually maintain definitions of all services, including descriptions, what services will be standardized, what services require a custom solution, and what services and components can be requested through each medium (e.g. Service Desk, Portal, Service Catalog, RFS).

   5.3. Establish and continually maintain Authorized Users lists on who is authorized to make Service Requests and what requests they are entitled to make.

   5.4. Communication to DIR and DIR Customers on the definition of services, the Request Management processes and changes thereto.

   5.5. Regular training for Authorized Users on Request Management processes, service definitions, and request mediums.

   5.6. Regularly collect feedback from Authorized Users on the effectiveness of Request Management, and engage in activities to improve.

6. Enable multiple mediums for accepting Service Requests, including the Service Desk, online Web portal, and Service Catalog.

   6.1. Enable the use of online self-service to allow Authorized Users to enter Service Requests through a “menu”-type selection, so that they can select and input details of Service Requests from a pre-defined list.

7. Develop and document processes and procedures regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may support the fulfillment of Service Requests.

8. Provide a mechanism for handling of Service Requests according to the agreed to prioritization model used by DIR, DIR Customers, and Third Party Vendor(s), as per processes described in the Request Management procedures, and appropriate SLAs.

9. Provide a mechanism for expedited handling of Service Requests that are of high business priority to DIR, DIR Customers, and Third Party Vendor(s), based on the assigned priority, as per escalation processes and procedures described in the Request Management processes.

10. Provide a mechanism for escalation of Service Requests that have missed or are at risk of missing expectations (e.g. fulfilment date, request scope, or other commitments), as per processes described in the Request Management processes and procedures.

11. Provide for real-time visibility of data records associated with Service Requests.

12. Update required information on Service Requests within designated timeframes to support an up-to-date accurate view of Service Requests.

13. Ensure proper approval (including any financial costs) associated with the Service Request (through automated means where practical) prior to Service Request fulfillment.

14. Develop, utilize, manage and continually improve an inventory of defined and documented Service Request models that incorporate at a minimum the following elements:

    14.1. Sequences of tasks, actions or steps to execute the Service Request Model and fulfill the Service Request.

    14.2. Identification of required dependencies, data sources, etc. that must be considered in executing the Service Request Model.

    14.3. Definition of responsibilities and roles to execute the Service Request Model.

    14.4. Timescales, milestones and thresholds for executing the Service Request Model.

    14.5. Anticipated escalation points and escalation procedures associated with the Service Request Model.

    14.6. Tasks, activities, methods, tools, systems, etc. to ensure that detailed audit information be recorded of all activity that creates, changes, or deletes data and user access to Service Provider systems that contain DIR and DIR Customer data.

15. Provide effective training on the purpose, activities, procedures, tools, policies, interfaces, etc. for all stakeholders to ensure effective execution of the process.

16. Provide and maintain regular communications between all parties and Authorized Users as required until Service Request completion and document the communications as per the Request Management processes.

    16.1. The frequency of such communications shall be determined by the severity of the request and in compliance with Service Request policies and procedures.

17. Keep DIR and DIR Customer informed of any issues with the completion of Service Requests and status changes throughout the Service Request life cycle and in accordance with agreed Service Levels.

18. Provide anticipated completion times for active Service Requests and update notification systems as required in the Request Management processes to keep DIR Customers and Authorized Users informed.

19. Ensure consistent ownership of the Service Request from recording to completion.

20. Review Service Request prior to closure to ensure proper categorization, documentation, confirmation of completion and activities required to initiated appropriate actions / processes / procedures (e.g. configuration information updates, etc.).

21. Close a Service Requests, per Service Management Manual guideline, after receiving confirmation from the requesting Authorized User or Service Provider support personnel for Service Request reported via a request submission system, that the Service Request has been completed.

    21.1. Follow Service Management Manual guidelines for closure where Authorized Users confirmation has not been received.

22. Track the progress of fulfillment efforts and the status of all Service Requests, including:

    22.1. Review the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.

22.2. Provide regular updates within designated timeframes as to the status of all Service Requests.

22.3. Coordinate Service Request tracking efforts, and provide and maintain regular communications, per the Service Management Manual, between all parties and Authorized Users until Service Request completion.

22.4. Keep the DIR Customer and Authorized User informed of changes in Service Request status throughout the Service Request life cycle in accordance with agreed Service Levels.

22.5. Keep DIR Customer informed of anticipated Service Request completion times for active Service Requests.

22.6. When a Service Request cannot be completed in the committed timeframe, provide a revised completion time or request a meeting with the Authorized User to determine a new timeframe.

22.6.1. Track all Service Request completions against the original committed timeframe, regardless of any revisions.

23. Leverage a knowledge base to assist with the fulfillment of Service Requests, including:

23.1. Make the knowledge base available online to Authorized Users for self-service.

23.2. Track the use of the knowledge base to report usage statistics.

24. Where Service Requests relate to the move of Assets, update details in the Asset Inventory and Management System and the CMS / CMDB, or coordinate with the relevant process to confirm updates are made.

25. Ensure that Service Requests follow the Change Management process as appropriate.

26. Where Service Requests require the changing of software assets update the Definitive Media Library (DML) or coordinate with the relevant process to confirm updates are made.

27. Ensure the additions or removals of assets are fulfilled in compliance with requirements for Redeployment and Disposal of Equipment.

A.1.7.2 Request Management System

Service Provider will utilize a Request Management System that provides a level of sophistication to promote the fulfillment of Requests associated with the Services within designated timeframes that accurately prioritizes and coordinates fulfillment efforts according to the business need of DIR and DIR Customers, and generally promotes good customer service and expectation setting.

Service Provider’s responsibilities include:

1. Implement an automated Request Management System, including the integration of applicable software, equipment, email, telephony, and Web technologies.

2. Receive and record all Service Request (including submissions received by telephone, electronically, or other means approved by DIR) in a Service Request Record, including classification and initial support.

3. Utilize and update the Request Management System with all relevant information relating to a Service Request.

4. Maintain a central knowledge database used to capture, store, and retrieve information and solutions for reuse by Service Provider personnel, other Service Component Provider(s), authorized Third Party Vendor(s), and Authorized Users.

   4.1. This central knowledge database shall enable the sharing of policies, procedures, best practices, and methods to fulfilling Requests among Service Provider personnel, other Service Component Provider(s), authorized Third Party Vendors(s), and Authorized Users.

5. Integrate with other systems, including Incident Management, Change Management, Configuration Management, Release Management and Program Management.

6. Integrate with the Request Management systems of other Service Component Provider(s) and designated Third Party Vendors.

7. Provide access to the Request Management System to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors; including all appropriate and required licenses and/or interfaces.

   7.1. Enable interfaces to integrate with other Request Management systems of other Service Component Provider(s), DIR, DIR Customers and authorized Third Party Vendors, as directed by DIR.

   7.2. Provide customizable capability that allows different configurations of interfaces based on standard user profiles.

8. Grant DIR access to the database of the Request Management System, and allow DIR to monitor and view on an ongoing basis.

9. Limit access to the Request Management Systems to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

10. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the Request Management System.

11. The Request Management System shall:

    11.1. Securely segregate DIR and DIR Customer data so that it can be accessed only by those authorized to comply with Government security requirements and in accordance with DIR policy.

    11.2. Provide for the partitioning of DIR Customer information in management and reporting.

    11.3. Provide for granting additional access in support of other Authorized Users (e.g. Audits) upon the request and as directed by DIR.

    11.4. Provide information necessary to record, track, and support Request Management for each Request submitted, including at a minimum:

       11.4.1. Request Identifier

       11.4.2. Category (based on required categorization schema agreed with DIR and DIR Customer)

11.4.3. Prioritization (including impact and urgency, based on required prioritization schema agreed with DIR and DIR Customer)

11.4.4. Requested by (person, system, etc.)

11.4.5. Method of notification

11.4.6. Requested activity

11.4.7. Action taken to fulfill Request

11.4.8. Request receipt date/time

11.4.9. Initial committed time to fulfill Request, and separately record any revisions to committed timeframes

11.4.10.Request closure date/time

11.4.11.Escalation details

11.4.12.Expedite details

11.4.13.Other information as needed to support the Service Level metrics

11.4.14.Other information as needed to support reporting

11.5. Identify Authorized Users designated by DIR and DIR Customer.

11.6. Provide for logging all modifications to Request Records, to provide full tracking, audit trail and change control at the named-user level.

11.7. Provide functionality to manage information for each Request submitted to, and originating from, Service Provider.

11.8. Link multiple contacts pertaining to the same Service Request to the associated Service Request Record.

11.9. When multiple Service Requests pertain to the same essential work, link the multiple Service Request Records to a single Service Request.

12. Provide online reporting capability with reasonably current data (and with unrestricted query length and depth) for use by Authorized Users in the generation of sophisticated, custom reports.

13. Provide end-to-end traceability, even when transactions span across multiple Applications, systems components, or parties.

A.1.7.3 Service Request Reporting

Service Provider’s responsibilities include:

1. Provide a monthly report on use of the knowledge base to fulfil Service Requests.

2. Provide a monthly report, or more frequently as required by DIR, including:

2.1. Progress toward fulfillment and the status of all Service Requests.

2.2. Committed fulfillment timeframes, anticipated completion times, and status.

2.3. Ownership and activities toward fulfillment for all open Service Requests.

2.4. Changes in Service Request status throughout the Service Request lifecycle.

2.5. Categories of Service Requests, by DIR Customer.

3. Provide a monthly report on Service Provider and other Service Component Provider(s) staff activities on Service Requests.
4. Provide a monthly report on outstanding and aging Service Requests and the trends thereof.
5. Provide reports on all requesting mediums to show demand, forecasts on demand, trends, product health, spend, problem areas, and backlogs.
6. Provide reports on the effectiveness of the Request for Solution process, including: time-to-solution, time-to-respond, accuracy of proposals, accuracy of forecast and captured compared to canceled.

A.1.7.4 Request For Solution

Service Provider's responsibilities include and Service Provider shall do the following:

1. Effectively execute the Request for Solution processes and appropriate mechanisms for the fulfillment of complex requests, requiring design, price, solution and proposals; including appropriate communications to adequately set expectations and promote good customer service.
2. As appropriate, execute Request for Solution processes and mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution.
3. Ensure that requests are appropriate and within the scope of Services being supported.
   - 3.1. Requests for partially out-of-scope Services should be reviewed with DIR for guidance
   - 3.2. Validate that the requestor is authorized by the DIR Customer for the type and category of request.
   - 3.3. Route requests appropriately for requests that can be fulfilled through other means.
4. Validate that the request is understood and has adequate information from the DIR Customer to support in-take.
   - 4.1. Develop and utilize standard mechanisms as approved by DIR for in-take.
5. Apply identifiers, review requirements with the DIR Customer, identify the entity (Service Provider, DIR or other Third Party) with the majority responsibility to solution, and provide liaison and management over to that entity.
6. Enable requests that require the coordination of Services from multiple sources; such as other Service Component Providers, Third Party Vendors, DIR or DIR Customers.
7. Coordinate and lead ad hoc and standing meetings as required to review requests, gather requirements, solution and make proposals, with other Service Component Provider(s), DIR, DIR Customers, and other Third Party Vendors.
8. Establish working relationships with DIR Customers and Authorized Users to clarify and gather in-depth requirements.
9. Provide and coordinate the attendance of all necessary SMEs in solution and requirement gathering sessions.

10. Provide a timeframe for delivering a solution proposal once requirements are complete.
11. Provide a proposed approach to solution to DIR Customer as appropriate.
12. Work with additional Service Provider(s) and other Third Party Vendors as required to formulate a complete solution and proposal.
13. Ensure all requests are solutioned within the DIR approved architecture and standards.
14. Ensure all requests are solutioned within the security policies, procedures, and guidelines of DIR.
15. Ensure all requests are solutioned within the bounds and guidelines of Service Provider technical operations.
16. Provide a single proposal to DIR Customers, compiling and coordinate solution elements from other Service Component Provider(s) and other Third Party Vendors as appropriate.
    16.1. Develop and provide standard proposal mechanisms for use of other Service Component Provider(s), DIR and DIR Customers.
17. Provide proposals for DIR approval and DIR Customer approval.
18. Develop and rework proposal responses as needed.
19. Facilitate the appropriate close of requests (e.g. acceptance or rejection by the DIR Customer or the inability for a solution to be formed).
20. Gather and validate that the proposal acceptance comes from an appropriately authorized user.
21. Provide to DIR and DIR Customers status of all outstanding requests such that DIR Customers can emphasize their organizational priorities.
    21.1. Maintain prioritization on a weekly basis, through the proper Request Governance mechanism, DIR Customers may revise priorities.
22. Provide process and procedure for DIR and DIR Customers to escalate requests that require urgent attention.
23. Track the status of requests to support meaningful reporting, including time-to-solution, time-to-respond, accuracy of proposals, accuracy of forecast, and captured compared to canceled.
24. Initiate Program Management as appropriate upon proposal acceptance by DIR Customer.

A.2 Service Delivery Services

A.2.1 Availability Management

Availability Management will ensure that the level of service availability delivered in all Services is matched to or exceeds the current and future agreed needs of the business, in a cost-effective manner. Availability Management provides a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets are established, measured and achieved.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Availability Management.
3. Validate that the Availability Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider's Availability Management process with the Availability Management processes of other Service Component Provider(s), DIR and authorized Third Party Vendors, with and where the processes interact.
5. Integrate Service Provider's Availability Management process with the other Service Management processes, including Configuration Management, Service Level Management, Capacity Management, IT Service Continuity Management and Incident Management.
6. Coordinate Availability Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.
7. Conduct regularly scheduled Availability Management meetings.
   - 7.1. Document and publish Availability Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.
8. Communicate and coordinate the Availability Management Process within Service Provider's own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).
   - 8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Availability Management Process.
9. Define Availability Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Availability Management processes.
   - 9.1. Routinely verify the effective compliance with the Availability Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

10. Establish on-going Availability Management activities with DIR and DIR Customers in coordination with other Service Component Provider(s) and designated Third Party Vendors.

11. Create and maintain an Availability Plan that is agreed to by DIR.

    11.1. Routinely verify the effective execution of the Availability Plan, by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

12. Establish a single focal point for Availability considerations in order to minimize the probability of conflicting priorities.

A.2.1.1 General Availability Management

Service Provider's responsibilities include the following:

1. Implement the Availability Management Policies and procedures, including policies and procedures for the following:

    1.1. Methods, tools, roles and activities for defining service and component availability requirements.

    1.2. Methods, tools, roles and activities for monitoring, measuring and reporting service and component availability.

    1.3. The standard formula for measuring availability of services and components that is agreed to with DIR and DIR Customers.

    1.4. Methods, tools, roles and activities for evolving availability metrics where Service Levels are not meeting DIR or DIR Customer business goals.

    1.5. Contents and use of the Availability Plan.

2. Provide an Availability Management process that will meet the following objectives:

    2.1. Produce and maintain an appropriate and up-to-date Availability Plan that reflects the current and future needs of DIR and DIR Customers.

    2.2. Provide advice and guidance to DIR and DIR Customers and IT on all availability-related issues.

    2.3. Ensure that service availability achievements meet or exceed all their agreed targets, by managing services and resources-related availability performance.

    2.4. Assist with the diagnosis and resolution of availability related incidents and problems.

    2.5. Assess the impact of all changes on the Availability Plan and the performance and capacity of all services and resources.

    2.6. Monitor and report on the availability of all services and resources.

    2.7. Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.

3. Provide and manage an Availability Management process that will incorporate the following activities.

3.1. Determining the availability requirements for a new or enhanced IT service and formulating the availability and recovery design criteria for the supporting IT components.

3.2. Determining the impact arising from IT service and component failure in conjunction with IT Service Continuity Management (ITSCM) and, where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to DIR and DIR Customers.

3.3. Defining the targets for the availability of services in coordination with DIR and DIR Customers.

3.4. Defining the targets for the availability, reliability and maintainability for the IT infrastructure components that underpin the IT service to enable these to be documented and agreed within SLAs, OLAs and contracts.

3.5. Establishing measures and reporting of availability, reliability and maintainability that reflect DIR and DIR Customers and IT support organization perspectives.

3.6. Monitor, measure, analyze and report service and component availability.

3.7. Monitoring and provide trend analysis of the availability, reliability and maintainability of IT components.

3.8. Reviewing IT service and component availability and identifying unacceptable levels.

3.9. Investigating the underlying reasons for unacceptable availability, report and provide remediation plans.

3.10. Produce service improvement plans, as specified by DIR and DIR Customers, which address business forecasts for Availability and reliability, and capitalize on any technology Changes that may cost-effectively improve levels of Availability and reliability.

3.11. Provide early warning or advice to DIR and DIR Customers of potential or actual Availability and reliability issues. Service Provider will provide additional advice as the potential increases and as the potential for service disruptions becomes more imminent.

4. Operate and maintain the Availability Management process to implement, measure, and manage the Availability and reliability of the Services and to confirm that the levels of Availability and reliability consistently meet DIR’s and DIR Customers’ business requirements and objectives.

5. Optimize Availability by collecting, monitoring, analyzing, and reporting on all key elements of Availability.

6. Assist in expressing Availability requirements in business terms.

7. Predict and design the Services for expected levels of Availability and security.

8. Produce an Availability Plan (in conjunction with Capacity and Financial Management) that is agreed by DIR and that will incorporate the following:

8.1. The scope of the Availability Management process, in terms of the services supported, the systems, environments, Operations Documents, Equipment, Software and Applications, etc.

8.2. The policies and procedures that ensure the success of the Availability Management process.

8.3. The activities of the Availability Management process.

8.4. The roles and responsibilities of the Availability Management process.

8.5. The systems and tool that support the Availability Management process.

8.6. Integration with and relationships with other Service Management processes, including Refresh, Transition and Transformation planning.

8.7. How the success of the process will be monitored, measured and reported.

8.8. Actual levels of availability provided versus agreed levels of availability for key IT services.

8.9. Availability measurements that are business- and customer-focused and which measure availability as experienced by the business and users.

8.10. Activities being progressed to address shortfalls in availability for existing IT services.

8.11. Where investment decisions are required, options with associated costs and benefits.

8.12. Details of changing availability requirements for existing IT services.

8.13. Options available to meet changed requirements, including the associated costs of each option.

8.14. Details of the availability requirements for new IT services.

8.15. Options available to meet these new requirements, including the associated costs of each option.

8.16. A forward-looking schedule for the planned availability analysis assignments.

8.17. A detailed description of the potential benefits and exploitation opportunities that exist for planned technology upgrades, including a description of anticipated availability benefits and the effort required to realize these benefits.

9. Measure and report availability of services in terms of business impact that are agreed by DIR and DIR Customers (e.g. user minutes lost, business transactions impacted, etc.).

10. Conduct detailed analysis of instances of unavailability and report findings to DIR using recognized analysis methods, such as Service Failure Analysis, Component Failure Impact Analysis, Fault Tree Analysis, Single Point of Failure analysis, modeling, etc.

11. Conduct Risk Analysis and Management to identify and quantify risks and justifiable countermeasures that can be implemented to protect the availability of IT systems.

12. Establish, execute and manage a testing schedule for Availability Management.

13. Provide and update a Projected Service Outage document (in conjunction with the Change Management process) which defines and sets out details regarding forward schedule of Changes, Releases, projects and other projected service downtime, and make these available through to DIR and DIR Customers.

14. Routinely review and improve Availability.

15. Provide the levels of Availability and reliability of the Services in compliance with the Service Levels, at optimum cost. The architecture should provide for scalability and the introduction of new layers of complexity that do not compromise overall reliability.
16. Produce service improvement plans, as specified by DIR and DIR Customers, which address business forecasts for Availability and reliability, and capitalize on any technology Changes that may cost-effectively improve levels of Availability and reliability.
17. Implement the service improvement plans after their approval by DIR and DIR Customers.
18. Produce Availability and reliability impact assessments with respect to Requests for Change and Work Orders in accordance with Service Levels.
19. Produce Availability and reliability trend analyses.
20. Manage the monthly number of Availability-related Incidents to trend downwards each year in accordance with the Service Levels.
21. Cooperate with DIR, DIR Customers and Third Party Vendor(s) to provide end-to-end Availability and reliability of the Services to Authorized Users.
22. Retain at least twenty-four (24) months of Availability and reliability source data or in compliance with the Customer Data Retention Schedule to enable trend analysis and to make such data available to DIR and DIR Customers.
23. Provide early warning or advice to DIR and DIR Customers of potential or actual Availability and reliability issues. Service Provider will provide additional advice as the potential increases and as the threat becomes more imminent.

A.2.1.2 Availability Management Reporting

Service Provider’s responsibilities include the following:

1. Provide regular reporting of service Outages related to the Services that affect Authorized Users irrespective of where the Outage occurred.
2. Provide a monthly report in a format agreed upon with DIR that, at a minimum, includes the following:
   - 2.1. Compare performance and Availability statistics for each Application/environment with planned performance and Availability.
   - 2.2. Provide a list of all Outages by DIR Customer, linked to an Incident, including the date and time the Outage commenced, its duration, and the affected infrastructure and Applications.
3. Provide trend analysis of the performance for each Application and Environment during the thirteen (13) most recent months Report on proposed preventative maintenance activities. Provide DIR with recommendations of preventative maintenance options.
4. Provide regular reporting with respect to the following measures for all services and components for both current reporting period and trend over the prior twenty-four (24) months, and make available through the Portal:
   - 4.1. Number and impact of instances of unavailability.

4.2. Mean time to restore.

4.3. Mean time between Service/System Incidents.

4.4. Mean time between failure.

4.5. Cost and impact of unavailability.

5. Provide regular reporting on the Availability of Service Management Systems (e.g. Incident Management, Request Management, Capacity Management) and the impact on Service Provider(s) ability to provide Services.

A.2.2 Capacity Management

Capacity Management will assess the business requirements (the required service delivery), the organization’s operation (the current service delivery), the IT infrastructure (the means of service delivery), and will ensure that capacity in all areas of IT service provision and support always exists and is matched to the current and future agreed needs of the business, within designated timeframes.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes and procedures with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Capacity Management.
3. Validate that the Capacity Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider’s Capacity Management process with the Capacity Management processes of other Service Component Provider(s), DIR and authorized Third Party Vendors, with and where the processes interact.
5. Integrate Service Provider’s Capacity Management process with the other Service Management processes, including Service Level Management, Availability Management, IT Service Continuity Management and Financial Management.
6. Coordinate Capacity Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.
7. Conduct regularly scheduled Capacity Management meetings.

7.1. Document and publish Capacity Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.

8. Communicate and coordinate the Capacity Management Process within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Capacity Management processes.

9. Facilitate and lead in the definition and documentation of Capacity Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Capacity Management processes.
    - 9.1. Routinely verify the effective compliance with the Capacity Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.
10. Establish on-going Capacity Planning activities with DIR and DIR Customers in coordination with other Service Component Provider(s) and designated Third Party Vendors.
11. Create, maintain and effectively execute the Capacity Plan that is agreed to by DIR.
    - 11.1. Continually verify the effective execution of the Capacity Plan, by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.
12. Establish a single focal point for Capacity considerations in order to minimize the probability of conflicting priorities.
13. Establish processes and procedures for forecasting DIR and DIR capacity requirements and in coordination with other Service Component Provider(s) and designated Third Party Vendors.
14. Lead demand management activities to encourage Authorized Users to make the most efficient use of the Services and to assist DIR and DIR Customers to minimize its costs while maximizing the value it receives from the Services.
    - 14.1. Develop demand management models and make recommendations to dampen Authorized User demands on systems, when requested by DIR.

A.2.2.1 General Capacity Management

Service Provider’s responsibilities include:

1. Service Provider will apply Capacity Management to all aspects of the Services.
2. Implement Capacity Management Policies and procedures, including policies and procedures for the following:
    - 2.1. Methods, tools, roles and activities for defining requirements for business capacity, service capacity and component capacity.
    - 2.2. Methods, tools, roles and activities for monitoring, measuring and reporting on business capacity, service capacity and component capacity.
    - 2.3. Standard formula for measuring the Capacity that is agreed to with DIR and DIR’s customers.
    - 2.4. Methods, tools, roles and activities for evolving capacity metrics where Capacity Management is not meeting DIR Customer business goals.
    - 2.5. Contents and use of the Capacity Plan.
3. Implement and manage a Capacity Management process that will meet the following objectives:
    - 3.1. Produce and maintain a Capacity Plan.

3.2. Measure the effectiveness of the Capacity Plan and relate implementations in meeting DIR and DIR Customer forecasts.

3.3. Provide advice and guidance to DIR and DIR Customers and IT on all capacity - related issues.

3.4. Ensure that service capacity achievements meet or exceed all their agreed targets, by managing services and resources-related capacity performance.

3.5. Assist with the diagnosis and resolution of capacity-related incidents and problems.

3.6. Assess the impact of all changes on the Capacity Plan and the performance and capacity of all services and resources.

3.7. Monitor and report on the capacity of all services and resources in accordance with the Service Management Manual.

3.8. Ensure that proactive measures to improve the capacity of services are implemented wherever it is cost-justifiable to do so.

3.9. Pre-empting performance issues by taking the necessary actions before they occur.

3.10. Producing trends of the current component utilization and estimating the future requirements, using trends and thresholds for planning upgrades and enhancements.

3.11. Modeling and trending the predicted changes in IT services, and identifying the changes that need to be made to services and components of the IT infrastructure and Applications to ensure that appropriate resource is available.

3.12. Ensuring that Service Provider upgrades are budgeted, planned and implemented before SLAs and service targets are breached or performance issues occur.

3.13. Tuning and optimizing the performance of services and components.

3.14. Monitoring, measuring, reporting and reviewing the current performance of both services and components.

3.15. Responding to all capacity-related “threshold” events and instigating corrective action.

3.16. Reacting to and assisting with specific performance issues.

4. Formally review capacity requirements as part of DIR’s normal business planning cycle.

5. Verify that there is adequate IT capacity to meet the required levels of service.

6. Manage IT capacity to meet demand for the Services.

7. Work with DIR Governance to achieve optimal utilization of IT capacity.

8. Provide additional capacity or advise DIR regarding the need for additional capacity, as appropriate.

9. Monitor resources and system performance, system utilization, capacity limits, and expected capacity needs, and record that information in the Capacity Management Information System (CMIS).

10. Determine capacity requirements of all new systems to determine the necessary computer and network resources required, and then size such new systems taking into account hardware utilization, performance Service Levels, and cost (minimizing cost to DIR and DIR Customers).

11. Utilize new hardware and software products in Capacity Management in order to improve the efficiency and effectiveness of the process, as part of the continuous improvement and evolution of the Services.

12. Carry out performance testing of Service Provider systems to confirm that such systems meet planned performance and utilization expectations and requirements.

13. As requested by DIR, DIR Customers, or as needed to deliver the Services, propose Service Levels that are maintainable and cost-justified.

14. Tune systems to achieve optimum use of all hardware and system software resources; ensuring that all changes are managed through the Change Management process.

15. Perform ad hoc performance and capacity studies as requested by DIR, DIR Customers, or as needed to deliver the Services.

16. In support of Application Development and Maintenance (ADM) activities, estimate applicable resource requirements, including impact on the capacity of the server environment, network environment, end-user computing environment, etc., as required.

17. Deploy proactive Capacity Management processes wherever practicable to do the following:

    17.1. Prevent Incidents and Problems related to resource utilization from occurring.

    17.2. Trend current system and resource utilization, and estimate future utilization.

    17.3. Validate and verify that planned changes affect only the foreseen resource impact.

18. Utilize reactive Capacity Management whenever necessary to facilitate successful performance of the Services.

19. Monitor new technology applicable to the Services and incorporate technological development, advances, and evolution into the Services.

20. Align Capacity Management with DIR’s Long-Range IT Plan.

21. Apply Capacity Management’s tools, data, reports, and disciplines to Incident and Problem relating to poor performance as an active member of teams working to resolve such Incidents and Problems.

22. Align Capacity Management outputs with the Service Levels and other performance requirements documented in the Agreement.

23. Actively include Capacity Management in the Change Management process to assess all changes for their impact on the capacity of the systems and provide appropriate feedback to those submitting changes.

24. Incorporate work schedules, seasonal workloads and dependencies between elements of the Services into Capacity Management planning.

25. Perform short-term demand management as required to maintain delivery of the Services during failures, spikes in demand, or other spontaneous events.

A.2.2.2 Capacity Planning

Service Provider’s responsibilities include:

1. Implement on-going activities with DIR and DIR Customers for Capacity Planning based on the documented Capacity Plan and coordinate with other Service Component Provider(s) and designated Third Party Vendors.
2. Incorporate appropriate capacity modeling to develop and deliver forecasts of growth and other changes in response to the projected DIR and DIR Customer business and operational needs disclosed by DIR to Service Provider.
    - 2.1. Use appropriate types of modeling (e.g. Pilots, Benchmarks, Prototypes, Baseline, Trends) along with current and historical resource utilization experience in support of business planning, IT planning, and capacity and utilization studies.
    - 2.2. Measure the effectiveness of the capacity planning models.
    - 2.3. On an agreed schedule, or as requested by DIR, revise the capacity planning model based on actual performance.
3. Forecast DIR’s capacity requirements through trending and monitoring and validate the capacity forecast, for DIR designated resources, against DIR’s actual utilization, by DIR Customer and Application.
4. Collect and establish with DIR and DIR Customers appropriate thresholds for supporting the demand and capacity monitoring.
5. Develop forecasts of growth and other changes in demand in cooperation with other Service Component Provider(s), DIR and DIR Customers, taking into account:
    - 5.1. Projected DIR and DIR Customers business and operational needs disclosed by DIR to Service Provider.
    - 5.2. DIR and DIR Customers’ business strategies, business plans, and financial plans.
6. Maintain a knowledge-base of future demand for the Services, and predict the effects of demand on Service Levels.
7. Validate that Capacity Planning appropriately supports the forecasts of growth or other changes in demand.
8. Conduct at least quarterly meetings with DIR Customers on Capacity Planning, and coordinate participation from other Service Component Provider(s) as necessary.
9. Coordinate and provide meaningful Capacity Planning input to the Technology Plan in support of requirements for Long-Range Planning.
10. Coordinate and provide meaningful Capacity Planning input to the Refresh Plan in support of Refresh and Technical Currency.

A.2.2.3 The Capacity Plan

The Capacity Plan will document the current levels of resource utilization and Service performance, and forecast future requirements accounting for DIR and DIR Customers’ business strategies and plans. The plan must clearly document assumptions and include recommendations quantified in terms of resources required, costs, benefits, impact, etc.

Service Provider’s responsibilities include the following:

1. The Capacity Plan will at a minimum include the following:

   1.1. An Introduction section which briefly explains the background to the current capacity issues, how the Capacity Plan was produced and what it contains, including the following:

   1.1.1. The current services, technology and resources.

   1.1.2. The organization's current levels of capacity.

   1.1.3. Problems being experienced or envisaged due to over or under-capacity.

   1.1.4. The degree to which service levels are being achieved.

   1.1.5. Changes made since the last issuance of the plan.

   1.2. A Management Summary which highlights the main issues, options, recommendations and analysis of costs to benefit.

   1.3. A description of the Business Scenarios (both current and future) that have been accounted for in planning capacity, including the anticipated growth in existing services, the potential new services and existing services scheduled for closure.

   1.4. A description of the scope and terms of reference for the Capacity Plan.

   1.5. A description of the methods used in obtaining information for all sub-processes of the Capacity Management Process – Business Capacity Management, Service Capacity Management, and Component Capacity Management.

   1.6. A description of the assumptions made in executing all sub-processes of the Capacity Management Process – Business Capacity Management, Service Capacity Management, and Component Capacity Management.

   1.7. A service summary that articulates the following:

   1.7.1. A service profile regarding the current and recent service provision for each service that is delivered, including throughput rates and the resulting resource utilization in light of short-, medium- and long-term trends.

   1.7.2. Service forecasts that include details of the new services planned and the growth or reduction in the use of existing services.

   1.8. A resource summary that articulates the following:

   1.8.1. A description of current and recent resource usage that concentrates on the resource usage by the services in light of short-, medium- and long-term trends in resource usage, broken down by system as gathered and analyzed by the sub-processes of Service Capacity Management and Component Capacity Management.

   1.8.2. Resource forecasts that include forecasts of the likely resource usage resulting from the service forecasts that address the business scenario mentioned in service forecasts.

   1.8.3. A description of possible options for improving the effectiveness and efficiency of service delivery.

2. Produce or update the Capacity Plan on a rolling annual schedule in conjunction with DIR's and DIR Customers' business planning cycle.

3. Incorporate DIR's and DIR Customers' capacity planning recommendations into the Capacity Plan.

4. Be forward-looking by eighteen (18) months unless otherwise specified by DIR.

A.2.2.4 Capacity Management Information System (CMIS)

Service Provider's responsibilities include the following:

1. Provide and maintain a CMIS that will serve as the single source of information regarding Capacity for Service Provider Services, other Service Component Provider(s) Services, and designated Third Party Vendors.

   1.1. Provide access to the CMIS to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors; which access shall include all appropriate and required licenses and/or interfaces.

2. Integrate the CMIS with other systems for Service Management, including Configuration Management, Service Level Management, Availability Management, IT Services Continuity Management and Financial Management.

3. Integrate the CMIS with the Capacity Management Information Systems of other Service Component Provider(s) and designated Third Party Vendors.

   3.1. Enable interfaces to integrate with the Capacity Management Information Systems of other Service Component Provider(s), DIR, DIR Customers and authorized Third Party Vendors, as directed by DIR.

4. Limit access to the CMIS to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

   4.1. Provide a mechanism or interface to allow DIR and DIR Customers to add their own capacity information, and modify/delete those entries.

   4.2. Provide a customizable set of views for different stakeholders through the service lifecycle.

5. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the CMIS.

6. Grant DIR and DIR Customer access to the database(s) of the CMIS and allow DIR to monitor and view on an ongoing basis.

7. The CMIS will contain data and information for:

   7.1. Service data (e.g. transaction response times or batch job execution times).

   7.2. Technical data (e.g. the maximum level of CPU utilization or the physical capacity of a particular hard disk).

   7.3. Financial data (e.g. the cost of new hardware or software components).

   7.4. Utilization data (e.g. CPU utilization, paging rates, or bandwidth utilization).

   7.5. Service performance information.

   7.6. Workload analysis information.

   7.7. Information regarding thresholds, events and alerts.

   7.8. Establishing relationships between dependent items or items with affinities.

   7.9. Identifying items by DIR Customer and any associated Service Provider or Third Party Vendor.

7.10. Identifying items by Application, software and/or service.

8. Update the CMIS within designated timeframes with the capacity information (technical capacity, thresholds, forecasts) newly acquired items, changed items and any other relevant information.

9. Maintain the CMIS to meet performance standards, to maximize efficiency, and to minimize outages, as necessary.

    9.1. Designate performance standards for the CMIS in the Service Management Manual.

10. The CMIS process and procedures will be implemented, maintained and updated, to ensure that recovery from an outage or corruption can be performed within designated timeframes to meet DIR and DIR Customers' business requirements.

11. Provide CMIS physical database management support, including providing backups and restores of data within designated timeframes.

12. Install, maintain, and support CMIS related database Software products.

13. Test and implement CMIS database environment changes, as approved by DIR.

14. Proactively provide capacity planning for the CMIS to prevent situations caused by lack of capacity (i.e. dataset or table space capacity events, full log files, etc.).

15. Correct situations caused by lack of CMIS within designated timeframes (e.g. dataset or table space capacity events, full log files, etc.).

A.2.2.5 Business Capacity Management

DIR employs business Capacity Management to facilitate alignment between its future IT requirements and future business requirements.

Service Provider's responsibilities include the following:

1. Service Provider will participate as needed in DIR's business Capacity Management planning processes.

2. Service Provider's participation in business Capacity Management will be sufficiently responsive so as not to impede DIR and DIR Customers' normal business planning cycles.

3. As part of DIR's SLA management, as requested by DIR, Service Provider shall provide DIR with the following:

    3.1. Assist with aligned Service Level Requirements.

    3.2. Verify SLA requirements for achievable targets.

    3.3. Design, procure or amend service configuration.

    3.4. Support SLA negotiation.

    3.5. Control and implementation through change management processes.

A.2.2.6 Service Capacity Management

Service Provider is responsible to DIR and DIR Customers for service Capacity Management (the management of the performance and capacity of the Services, as used by Authorized Users).

Service Provider’s responsibilities include the following:

1. The management, control and prediction of the end-to-end performance and capacity of the production Services usage and workload.
2. Ensure that the performance of all Services, as detailed in service targets within SLAs and SLRs, is monitored and measured, and that the collected data is recorded, analyzed and reported.
3. Wherever necessary, instigate proactive and reactive action to ensure that the performance of all services meets their agreed business targets.
4. Use automated thresholds to manage all operational services, to ensure that situations where service targets are breached or threatened are rapidly identified and cost-effective actions implemented to reduce or avoid their potential impact.
5. Investigate and research threshold breaches and near misses to determine what remedial action should be taken; then plan and perform such remedial actions through the Change Management Process.
6. Employ regular monitoring, identification of exceptions, and manual review of reports and trends.

A.2.2.7 Component Capacity Management

Service Provider is responsible for Component Capacity Management (the management of the performance and capacity of the components comprising the Services).

Service Provider’s responsibilities include the following:

1. The management, control and prediction of the performance, utilization and capacity of individual IT components within the Service.
2. Ensure that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analyzed and reported.
3. Use automated tools to manage thresholds of all components.
4. Ensure that situations where service targets are breached or threatened by component usage or performance are rapidly identified, and cost-effective actions to reduce or avoid their potential impact are implemented.
5. Maintain an understanding of the capacity and utilization of each of the IT components that Service Provider manages, including hardware, software licenses, and voice and data circuits.
6. As necessary to provide optimum resource usage (hardware, software, circuits, etc) in the delivery of the Services, install hardware and software monitors, properly configure those monitors, and collect the resultant data.
7. Upon request, estimate the resource and utilization effects of planned changes.
8. Respond in an effective manner and within designated timeframes to Incidents and Problems that are caused by a lack of resource or an inefficient use of a resource.
9. Proactively identify components that are susceptible to failure, and recommend cost-effective solutions for DIR’s and DIR Customers’ consideration and possible approval; including performance improvement expectations.

10. Upgrade, remove, or add capacity as otherwise necessary to meet DIR and DIR Customer requirements, or proactively recommend capacity changes where Service Provider is not financially responsible for a specific component.

A.2.2.8 Capacity Management Reporting

Service Provider's responsibilities include the following:

1. Provide monthly regular reporting of activities against the Capacity Plan.
2. Publish regular Capacity Management reports to DIR Customers, which at a minimum will include current/recent utilization (and trends) compared to normal utilization, Service Levels, and previously identified baselines.
3. Produce monthly reports on the current usage of resources, trends and forecasts and exceptions, in a format agreed to by DIR, that at a minimum includes the following:
   - 3.1. Business Capacity reports based on current performance compared to thresholds and forecast.
   - 3.2. Service Capacity reports based on current performance compared to thresholds and forecast.
   - 3.3. Component Capacity reports based on current performance compared to thresholds and forecast.
   - 3.4. Capacity-related Incidents and Problems
   - 3.5. Outstanding capacity improvements.
   - 3.6. Trend analysis of current performance.
4. Provide a mechanism for DIR and DIR Customer to report against the CMIS data.
5. Provide regular reporting on the Capacity of Service Management Systems (e.g. Incident Management, Request Management, Asset Management) and the impact on Service Provider(s) ability to provide Services.

A.2.3 Service Level Management

Service Level Management will maintain and gradually improve business-aligned IT service quality through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service according to the Severity Levels, as described in **Attachment 3-E**. Service Provider will provide Service Level Management as described in **Exhibit 3**.

A.2.4 IT Service Continuity Management

IT Service Continuity Management will support the overall Business Continuity and Disaster Recovery process by ensuring that the required IT technical and services operations (including computer systems, networks, Applications, data repositories, telecommunications, environment, technical support and Service Desk) can be recovered within required and agreed business time scales. Service Provider must provide IT Service Continuity Management as described in this **Exhibit 2.1** and **Exhibit 15** and **Exhibit 16**.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes and procedures with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end IT Service Continuity Management.
3. Validate that the IT Service Continuity Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider’s IT Service Continuity Management process with the IT Service Continuity Management processes of other Service Component Provider(s), DIR and authorized Third Party Vendors, with and where the processes interact.
5. Integrate Service Provider’s IT Service Continuity Management process with the other Service Management processes, including Service Level Management, Availability Management, Capacity Management, Configuration Management, Change Management and Incident Management.
6. Coordinate IT Service Continuity Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.
7. Conduct regularly scheduled IT Service Continuity Management meetings.
   7.1. Document and publish IT Service Continuity Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, Service Component Providers and authorized Third Party Vendors.
8. Communicate and coordinate the IT Service Continuity Management Process within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).
   8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the IT Service Continuity Management processes.
9. Facilitate and lead in the definition and documentation of IT Service Continuity Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the IT Service Continuity Management processes.
   9.1. Continually verify the effective compliance with the IT Service Continuity Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.
10. Establish on-going IT Service Continuity Planning activities with DIR and DIR Customers in coordination with other Service Component Provider(s) and designated Third Party Vendors.
11. Create, maintain and effectively execute the IT Service Continuity Plan that is agreed to by DIR.
    11.1. Continually verify the effective execution of the IT Service Continuity Plan, by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

12. Establish a single focal point for IT Service Continuity considerations in order to minimize the probability of conflicting priorities.

13. Develop and manage IT Service Continuity Management processes that will include the following:

    13.1. Developing and maintaining IT Service Continuity Plans and IT Recovery Plans for DIR and DIR Customers.

    13.2. Conducting regular testing of plans, including Business Impact Analysis (BIA) exercises and Risk Analysis and Management exercises, for DIR and DIR Customers.

    13.3. Conducting Risk Analysis (RA) for DIR and DIR Customers – the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality, in relation with DIR and DIR Customers (as outlined in **Exhibit 6**). This also includes taking measures to manage the identified threats where this can be cost-justified with DIR and DIR Customer.

    13.4. Producing an overall ITSCM strategy that must be integrated into the BCM strategy, which should include elements of risk reduction as well as selection of appropriate and comprehensive recovery options.

14. Following any disaster, conduct a post-disaster meeting with other Service Component Provider(s), DIR and DIR Customers in order to understand the cause of the disaster; and develop plans to eliminate or mitigate future occurrences.

A.2.4.1 General IT Service Continuity Management

Service Provider's responsibilities include the following:

1. Effectively implement IT Service Continuity Management Policies and procedures, which at a minimum include the following:

1.1. Scope, methods, roles and activities for defining requirements for IT Service Continuity Plans and IT Recovery Plans.

1.2. Standard contents and use of IT Service Continuity Plans and IT Recovery Plans.

1.3. Standard methods, tools, roles and activities for effective Business Impact Analysis.

1.4. Standard methods, tools, roles and activities for engaging DIR Customers on ITSCM and conducting exercises.

1.5. Methods, tools, roles and activities for monitoring and reporting on ITSCM activity.

1.6. Methods, tools, roles and activities for evolving metrics where ITSCM is not meeting DIR Customer business goals.

2. Effectively execute the IT Service Continuity Management processes, include the following:

    2.1. Actively participate in maintaining a set of IT Service Continuity Plans and IT recovery plans that support the overall Business Continuity Plans (BCPs) of DIR and DIR Customers

    2.2. Participate in regular testing of the plans.

2.3. Participate in ongoing operation and maintenance of the plans.

2.4. Participate in regular BIA exercises to verify that all continuity plans are properly maintained with changing business impacts and requirements, and to identify and report to DIR and DIR Customers where plans are out of compliance.

2.5. Participate in regular Risk Analysis and Management exercises, particularly in conjunction with the business and the Availability Management and Security Management processes, that manage IT services within an agreed level of business risk.

2.6. Provide advice and guidance to all other areas of the business and IT on all continuity- and recovery-related issues

2.7. Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed Services elements for business continuity targets of DIR Customers.

2.8. Assess the impact of all changes on the IT Service Continuity Plans and IT Recovery Plans and provide reports on the assessed impact.

2.9. Verify that the DCS Service Providers have the necessary contracts with Third Party Vendors for the provision of the necessary recovery capability to support all IT Service Continuity Plans.

A.2.4.2 Business Continuity

DIR and DIR Customers will retain responsibility for their Business Continuity plans and management activities.

Service Provider responsibilities include:

1. Update, maintain, manage, test and implement any portion of the Business Continuity plans and activities that relate to the continued provision of the Services.
2. Ensure that there is the proper linkage between the Business Continuity Plan and Disaster Recovery Plan to make them holistic and integrated.
3. Comply with TAC 202 requirements for all Business Continuity items related to security.

A.2.4.3 Disaster Recovery Planning

MSI will have responsibility for coordinating the development, maintenance, testing and in the event of a disaster the implementation of Disaster Recovery Plans at an Application, DIR Customer and DIR level.

Service Provider will be responsible for the development and modification of Disaster Recovery plans for the Services in coordination with DIR and DIR Customers. Such plans will be in compliance with **Exhibit 16** and the Disaster Recovery Priority established for each DIR Customer Application.

DIR and DIR Customers will approve Disaster Recovery plans and modifications to such plans.

Service Provider’s responsibilities include:

1. Effectively manage and maintain the Disaster Recovery plans of DIR and DIR Customers, as they exist on the Effective Date.

2. To the extent that DIR and DIR Customers do not have a documented Disaster Recovery plan encompassing all Services, Service Provider will develop and implement a Disaster Recovery plan using Service Provider’s best practices and standards for companies of similar industry, size, and services. DIR or DIR Customers will approve any such Disaster Recovery plan developed by Service Provider and will provide support in creating the plan.
3. Maintain and continually enhance DIR’s and DIR Customers’ Disaster Recovery plans throughout the term of the Agreement, including enhancements required due to the introduction and use of new technologies (Equipment, Software, Applications, etc.), Resource Units, processes, business functions, locations, and priorities.
4. Integrate the Disaster Recovery plans related to the Services with any DIR Customer Business Continuity plans and activities of DIR.
5. Integrate the Disaster Recovery plans related to the Services with the plans of any Third Party Vendors and any activities of Third Party Vendors associated with Disaster Recovery planning or Disaster Recover response.
6. Document the manner, processes and procedures by which Service Provider will perform backups, provide Disaster Recovery services, and assist with Business Continuity.
7. Document DIR Customers priorities for Disaster Recovery and Business Continuity based on the priorities established by DIR.
8. Document the methods, processes and timeframes that allow DIR Customers to change priorities, as specified in Service Management Manual.
9. With DIR and DIR Customer’s input and approval, develop a process that will determine and modify the list of mission-critical Applications on a continual basis with annual reviews.
10. Work with DIR and DIR Customers to incorporate security measures, as defined for normal operations, into the Disaster Recovery plans.
11. Maintain a list of key personnel contacts and notification procedures for DIR, DIR Customers, Service Provider, and Third Party Vendor personnel.
12. Comply with DIR’s definition and procedures for declaring a disaster.
13. Provide DIR with Service Provider’s criteria and procedures for declaring a disaster at Service Providers facilities.
14. Provide a single point of contact for Business Continuity and Disaster Recovery plans, related communications and other activities that are Service Provider’s responsibility.
15. Integrate the Disaster Recovery plans with the DIR Customer Business Continuity Plans related at a minimum to the following aspects:

    15.1. Emergency Response Plan.

    15.2. Damage Assessment Plan.

    15.3. Vital Records Plan.

    15.4. Crisis Management and Public Relations Plan.

    15.5. Security Plan.

    15.6. Personnel Plan.

15.7. Communication Plan.

15.8. Finance and Administration Plan.

16. Verify that DCS Service Providers are ensuring backups and off-site retentions for Application and System Software to support the RTO and RPO objectives for each DIR Customer Application.

A.2.4.4 Disaster Recovery Testing

Service Provider will be responsible for the development and modification of Disaster Recovery testing for the Services in coordination with DIR and DIR Customers. Such tests will be scheduled in compliance with **Exhibit 16**.

Service Provider's responsibilities include:

1. Establish joint test objectives with DIR and DIR Customers designed to verify that all systems will be available within an established timeframes.

   1.1. Provide for DIR and DIR Customer acceptance of test plan.

2. Schedule and test all components of the Disaster Recovery plans as required in cooperation with DIR and DIR Customers.

3. Schedule testing dates with DIR and DIR Customer's approval and give DIR and DIR Customers the opportunity to observe and participate in the tests.

   3.1. Record and report to DIR when a DIR Customer chooses not to test, including the identification of the affected DR Plans and Applications.

4. Assume coordination and administrative responsibility for Third Party Vendors utilized by DIR and DIR Customers during testing in accordance with the Disaster Recovery plans.

5. Continue to operate and manage the Services during periodic Disaster Recovery tests.

6. Provide DIR and DIR Customers with a formal report of the test results within thirty (30) days of each test. At a minimum, these reports should include:

   6.1. The results achieved.

   6.2. A comparison of the results to the measures and goals identified in the respective plans.

   6.3. A report on the feedback from Authorized Users as to the adequacy of continuity for their respective areas.

   6.4. A plan and a schedule to remedy any gaps revealed during testing.

   6.5. Through coordination with DIR Customer ensure that Application integrity exists after restoration in accordance with the formal DR Plan.

7. Retest within ninety (90) days if any disaster simulation(s) fails to achieve specified results as a result of Service Provider's failure to perform its responsibilities.

   7.1. Update the Disaster Recovery plans upon re-testing and verify that the remedy was successful.

A.2.4.5 Disaster Recovery Activities

Service Provider's responsibilities include:

1. Report disasters (or potential disasters) to DIR and DIR Customers immediately upon identification based on parameters defined in the Disaster Recovery plans, and consult with DIR for an official declaration of a disaster as appropriate.
2. For all facilities where Service Provider has oversight responsibility, declare disasters in accordance with procedures existing at the time of declaration and notify DIR and DIR Customers of situations that may escalate to disasters as soon as practicable.
3. Execute the Disaster Recovery plans including:
   - 3.1. Install or coordinate the installation of Equipment.
   - 3.2. Operate the Equipment.
   - 3.3. Restore the Software.
   - 3.4. Verify that data is recovered to the appropriate point in time.
   - 3.5. Provide all other functions associated with the Services.
   - 3.6. Support DIR Customers as required to bring Applications into production ready mode.
4. In accordance with the Disaster Recovery plans, determine what resources to deploy.
   - 4.1. Conduct, supervise, and administer the operation and implementation of such resources.
5. Provide additional resources as necessary to maintain provision of the Services for unaffected areas and re-align technical resources to maintain Business Continuity.
6. In accordance with the Disaster Recovery plans, assume coordination and administrative responsibility for Third Party Vendors utilized in the delivery of Services.
7. In accordance with the Disaster Recovery plans develop a plan for the return of Services to the original processing site or an alternate(s) site specified and agreed to by DIR in the Disaster Recovery plans.
8. Whether a Disaster Recovery plan exists or not, at a minimum, restore the Services within a timeframe that is expected in the industry from large, well-managed outsourcing services companies.
9. Provide for a return of readiness to respond to a Disaster, as set forth in the Disaster Recovery plans.

A.2.4.6 Other Disaster Recovery Activities

Service Provider's responsibilities include:

1. Negotiate and manage Service Providers contracts with Third Party Vendors providing Disaster Recovery services and validate and manage Service Component Providers contracts with Third Party Vendors providing Disaster Recovery services.
2. At all times, maintain strict compliance with the Disaster Recovery policies, standards, and procedures contained in DIR's and DIR Customers' Disaster Recovery plans.

3. Train Service Provider, DIR, DIR Customers and designated Third Party Vendor personnel in Disaster Recovery procedures, and implement a process to obtain immediate access to such procedures in a disaster situation.
4. Provide an effective program of on-going activities to support the Disaster Recovery Plan, including at a minimum the following:
   - 4.1. Conduct a regular review of all of the deliverables from the ITSCM process needs to be undertaken to ensure that they remain current.
   - 4.2. Establish and maintain an on-going program of regular testing to ensure that the critical components of the strategy are tested, arranged in line with business needs and the needs of the BCPs, and after every major business change.
   - 4.3. The backup and recovery of IT service should also be monitored and tested to ensure that when they are needed during a major incident, they will operate as needed.
5. Provide effective integration with the Change Management process to ensure that all changes are assessed for their potential impact on the ITSCM plans.
6. For Server and Mainframe Services, provide and maintain backups, file recovery capabilities, and historical files of data and Software (including source code) utilized to process data. Additional responsibilities will include the following:
   - 6.1. Adhere to the time periods specified for backups and recovery by DIR and DIR Customers in the Disaster Recovery plan.
   - 6.2. Use magnetic media or other media approved by DIR and accessible to DIR and DIR Customers.
   - 6.3. Provide off-site storage in a secure facility for the foregoing, as well as daily pickup and delivery to the off-site storage site.
   - 6.4. Perform such functions in accordance with standards and procedures in the Disaster Recovery plans, and being no less stringent than the standards and procedures used at well-managed companies that provide similar backup and recovery features for similar services.

A.2.5 IT Financial Management

Proper IT Financial Management will provide cost-effective stewardship of the IT assets and the financial resources used in providing IT Services. Service Provider must provide IT Financial Management Services as described in **Exhibit 4**.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes and procedures with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end IT Financial Management.
3. Validate that the IT Financial Management processes provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.

4. Integrate Service Provider's IT Financial Management process with the IT Financial Management processes of DIR and other Service Component Provider(s), as well as authorized Third Party Vendor(s)' IT Financial Management processes, with and where the processes interact.

5. Integrate Service Provider's IT Financial Management process with the other Service Management processes, including Service Level Management, Capacity Management, and Configuration Management, as well as areas of governance as described in **Exhibit 6**.

6. Coordinate IT Financial Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customers.

7. Conduct regularly scheduled IT Financial Management meetings, included those associated with the requirements for governance as described in **Exhibit 6**.

   7.1. Document and publish IT Financial Management meetings status reports to all relevant stakeholders.

8. Communicate and coordinate the IT Financial Management processes and policies within Service Provider's own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

9. Facilitate and lead in the definition and documentation of IT Financial Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the IT Financial Management process, as approved by DIR.

   9.1. Routinely verify the effective compliance with the IT Financial Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

A.2.5.1 Chargeback and Utilization Tracking System

Service Provider's responsibilities include:

1. Provide and maintain a Chargeback and Utilization Tracking System (Chargeback System) that will serve as the single source of information regarding all IT Financial information for Service Provider Services, other Service Component Provider(s) Services, and designated Third Party Vendors.

   1.1. Provide access to the Chargeback System to other Service Component Provider(s), DIR and DIR Customers, and authorized Third Party Vendors based on agreed Authorized User profiles (e.g. by DIR Customer); which access shall include all appropriate and required licenses and/or interfaces.

2. Integrate the Chargeback System with other systems for Service Management, including, but not limited to Service Level Management, Capacity Management (CMIS), and Configuration Management (CMS / CMDB).

3. Integrate the Chargeback System with the IT Financial Management Systems of other Service Component Provider(s) and designated Third Party Vendors.

3.1. Enable interfaces to integrate with the IT Financial Management Systems of other Service Component Provider(s), DIR and authorized Third Party Vendors, as directed by DIR.

4. Provide Service Provider, other Service Component Provider(s), DIR and DIR Customers and authorized Third Party Vendors with appropriate training in using the Chargeback System including ongoing training for new Authorized Users.

5. Grant DIR access to Chargeback System source data and any database(s), and allow DIR to monitor and validate on an ongoing basis.

6. Provide sufficient detail to support DIR and DIR Customers State and Federal funding accounting, grant and audit requirements.

7. The Chargeback System shall at a minimum support the following:

7.1. Web-based DIR and DIR Customer access, transaction and job drill down capability for all billing transactions , ad hoc query access, and soft copy billing downloads by any DIR Customer number, account code and/or resource unit identifier(s) combination.

7.2. Accounting, usage tracking, self-service cost allocation, rate setting, invoice validation, reporting to DIR and DIR Customers.

7.3. Collecting and aggregating billing, service provisioning, and service metric information from Service Provider Services, other Service Component Provider(s) Services, designated Third Party Vendors to DIR and DIR Customers including any DIR retained services.

7.4. Reports as described in **Exhibit 13** and ad hoc queries with appropriate local print formatting.

7.5. Unique DIR Customers account identifiers to identify Applications and other services information.

7.6. DIR and DIR Customers self-service access to input and maintain Account Code Identifiers and Structures with effective dates, Resource Unit unique identifiers and cost category mapping of accounting information at the lowest level of detail for Resource Units, New Services, One-Time Charges, and Pass-Through Expenses allowing for multiple lines of detail for multiple accounts and funding sources.

7.7. Electronic and hard copy chargeback detail as specified by DIR and DIR Customer.

7.8. Electronic monthly billing detail and accounts receivables detail in DIR approved formats.

7.9. Capability for DIR to access all billing and service information at summary and detail levels by DIR Customer and DIR Customer account and resource unit identifiers.

7.10. Capability for DIR Customers to access all billing and service information for their account identifier.

7.11. Providing multiple Service Provider billing information to DIR and DIR Customers with Base Charges, Pass-Through Expenses, One-Time Charges, and misc Labor Charges implemented and maintained in common formats.

8. Maintain Chargeback System to meet DIR approved performance standards for maximizing efficiency and to minimizing outages.

    8.1. Designate performance and disaster recovery standards for the Chargeback System in the Service Management Manual.

9. Develop, maintain, and implement DIR approved Chargeback System archive processes and procedures required to improve performance or recover from an outage or corruption within designated timeframes.

10. Provide Chargeback System physical database management support, including providing backups and data restores within designated timeframes.

11. Test and implement DIR approved Chargeback System database and environment changes.

12. Proactively provide Chargeback System capacity planning and implement corrective measures to prevent system performance degradation or outages (i.e. dataset or table space capacity events, full log files, etc.).

A.2.5.2 Chargeback and Utilization Reporting

Service Provider's responsibilities include:

1. Support all charges with detailed invoice reports in **Attachment 4-F** and supporting utilization data as described in **Attachment 13-A** at the DIR Customer, Resource Units, cost category (e.g. Programs, Divisions, Organization Units) and Resource Unit unique ID level, as required.

2. DIR Customers will identify unique Resource Unit IDs and provide cost category mapping through the self- service Portal.

3. Chargeback Service Provider billing will apply all changes to accounting information during the billing period.

A.2.5.3 Chargeback Invoice Consolidation

Service Provider's responsibilities include:

1. Provide DIR with a monthly invoice report that accounts for each DCS Service Provider and designated Third Party Vendors Charges.

2. Provide a single monthly chargeback invoice for each DIR Customer for all DCS Service Provider Services and any DIR retained service.

3. Provide DIR with a monthly report reconciling the total of all DIR Customer chargeback invoices with the cumulative total of each DCS Service Provider invoice.

4. Provide DIR with the supporting detail necessary to facilitate DIR's payment to all DCS Service Providers that are supplying Services under the Agreement.

5. Execute DIR-approved invoice validation process.

6. Report results of invoice validation process and identify anomalies based on DIR approved variance thresholds prior to the release of the DIR Customer chargeback invoices.

7. Provide DIR a monthly report that confirms amounts paid to each Service Provider and any outstanding balance that was not paid with sufficient detail for DIR to confirm the unpaid balances.

A.2.5.4 Invoice Dispute Processing

Service Provider’s responsibilities include:

1. Record, track and manage incidents of DIR and DIR Customer invoice disputes.
2. Research and review invoice disputes for completeness and supporting data accuracy and, when necessary, request clarifying data from DIR or DIR Customer.
3. Forward invoice disputes to the appropriate Service Component Provider(s) for processing within the agreed time lines.
4. Responsible for facilitating resolution of invoice disputes with all applicable Service Component Providers and DIR and DIR Customers within designated timeframes.
5. Ensure that incidents of invoice disputes are continually updated, at a minimum on a weekly basis.
6. On a weekly basis, provide DIR with invoice dispute metrics and dispute aging reports.
7. Where applicable, calculate and assess interest on other DCS Service Provider(s) for disputes resulting in credits to DIR and DIR Customers.
8. Provide a process for the resolution of invoice disputes.
9. Allow DIR to monitor and validate invoice dispute process on an ongoing basis.
10. Provide regular progress notifications to DIR and DIR Customers on outstanding incidents of invoice disputes, until the invoice dispute is resolved and in accordance with DIR policies.
11. Provide a process for escalating to Service Provider’s management incidents of invoice disputes not resolved within the time frames established within DIR policies.

A.2.6 Security Management

Service Provider's delivery of Security Management shall be an integral part of the other IT disciplines and deployed across all Service Components to ensure that requirements, as defined in **Exhibit 17**, are met and verified. Security Management shall assess all risks associated with the delivery of Services are appropriately identified, evaluated, assessed and appropriate controls are implemented and maintained.

Service Provider’s responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve end-to-end Security Management.
3. Validate that the Security Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.

4. Integrate Service Provider’s Security Management process, including Logical Security Administration, with the Security Management processes of other Service Component Provider(s), DIR and authorized Third Party Vendors, with and where the processes interact.

5. Integrate Service Provider’s Security Management process, including Logical Security Administration, with all the other Service Management processes, including Incident Management, Change Management, and IT Service Continuity Management, where the processes interact.

6. Coordinate Security Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.

7. Conduct regularly scheduled Security Management and Risk Management meetings.

    7.1. Document and publish meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.

8. Communicate and coordinate the Security Program and Security Management processes within Service Provider’s own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).

    8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Security Management processes.

9. Facilitate and lead in the definition and documentation of Security Management Policies and procedures, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Security Management processes.

    9.1. Continually verify the effective compliance with the Security Management Policies and procedures by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

10. Establish an on-going Security Program that accomplishes the goals for Security Management and coordinates the activities of DIR, DIR Customers, other Service Component Providers and designated Third Party Vendors.

11. Create, maintain and effectively execute the Security Plan, which is agreed to by DIR.

    11.1. Regularly verify the effective execution of the Security Plan, by Service Provider, other Service Component Provider(s), DIR Customers and designated Third Party Vendors.

12. Establish on-going Risk Management and assessment activities with DIR and DIR Customers in coordination with other Service Component Provider(s) and designated Third Party Vendors.

13. Establish a single focal point for Security and Risk mitigation considerations in order to minimize the probability of conflicting priorities.

14. Develop and manage Security Management processes and procedures and Risk Management processes and procedures.

A.2.6.1 General Security Management

Service Provider’s responsibilities include:

1. Meet the external requirements according to security policies, contractual requirements, legislative requirements, TAC 202, the requirements defined in **Exhibit 17** and as expressed in the Service Levels described in **Exhibit 3**.
2. Meet the internal security requirements according to internal security policies, standard security baselines, as expressed in the OLAs.
3. Develop, maintain, update, and implement security procedures with DIR and DIR Customer’s review and approval, including physical access strategies and standards.
4. Assist DIR and DIR Customers in implementing security requirements.
5. Meet all Security-related Service Levels as defined in **Exhibit 3**, which are to be agreed to by DIR and Service Provider.
6. Support planning activities, which includes creating the necessary contracts, OLAs, and policy statements.
7. Support implementation within the Services, which includes creating awareness; completing classifications and registrations; managing personnel security, physical security, and security for Equipment and Applications; controlling and managing Access Rights; and handling Security Incidents and registration with appropriate Security response group (e.g. CERT).
8. Provide command and control for response, which includes organizing, establishing a management framework, and allocating responsibilities.
9. Provide the environments (e.g. tools, processes, procedures, systems) for managing encryption keys used in support of the Services (e.g. infrastructure backup, DIR Customer Applications).
10. Provide for security evaluations, which include conducting internal audits, supporting external audits, conducting self-assessments, and evaluating security incidents.
11. Produce a Security Plan that is agreed by DIR and that will incorporate at a minimum the following:

    11.1. The scope of Security Management, in terms of the services supported, the systems, environments, Operations Documents, Equipment, Software and Applications, etc.

    11.2. The policies and procedures that ensure the success of the Security Management.

    11.3. The activities of the Security Management.

    11.4. The roles and responsibilities of Security Management.

    11.5. The systems and tool that support Security Management.

    11.6. Integration with and relationships with other Security Management.

    11.7. How the success of Security Management will be monitored, measured and reported.

    11.8. Provide for 24 x 7 security monitoring and reporting on Security events.

    11.9. Measure actual Security provided versus agreed levels of Security.

11.10. Provide Controlled Penetration Tests on Service Provider Systems at Service Provider Facilities.

11.11. Participate in DIR Controlled Penetration Tests.

11.12. Provide for vulnerability scans for all network assets, which should include scans for all network addresses at least once per year

11.13. Activities to address shortfalls in Security.

11.14. Where investment decisions are required, provide options with associated costs and benefits.

11.15. Options available to meet changed Security requirements, including the associated costs of each option.

11.16. Details of the Security requirements for new IT services, including options for meeting these requirements and any associated costs.

11.17. A forward-looking schedule for the planned Security testing, assessments and analysis.

11.18. A detailed description of the potential benefits and exploitation opportunities that exist for planned technology upgrades, including a description of anticipated Security benefits and the effort required to realize these benefits.

12. Provide reporting on security management and the execution of the Security Plan.

13. Regularly review, capture learning and improve on Security, and the execution of the Security Plan.

14. Vendor owned equipment and software in support of the agreement must comply with TAC 202 and applicable Texas Government Code, including the appropriate use of encryption and authentication controls.

15. Provide for and facilitate the annual risk assessment, in compliance with **Exhibit 17**.

A.2.6.2 Security Clearances

Service Provider's responsibilities include:

1. Service Provider personnel must have received security clearance, in accordance with the **Exhibit 17** and the Service Management Manual.
2. Establish and document processes and procedures for complying with the security clearance requirements, to include on-boarding and off-boarding processes and procedures.
3. Ensure that any Service Provider personnel with logical or physical access to DIR Facilities or Data has successfully obtained the appropriate security clearance.
4. Ensure that any Service Provider personnel that has not completed the security clearance requirements are escorted at all times while at DIR Facilities.
5. Implement processes and procedures for tracking clearances for all Service Provider personnel, other Service Component Providers, and Third Party Vendors.
6. Ensure that there is auditable tracking of access granted, logical security clearances and access revocations for all Service Provider personnel.

7. Track which individuals have been trained on the Security Program, and DIR and DIR Customer security policies and procedures as appropriate.
8. Report on the security clearances at DIR and DIR Customer request.
9. Provide physical and logical access reports as requested by DIR and DIR Customers.

A.2.6.3 Security Clearance Database

Service Provider's responsibilities include:

1. Provide and maintain a comprehensive database for tracking security clearances for all Service Provider personnel, other Service Component Provider(s), and designated Third Party Vendors.
    1.1. Provide access to the security clearance database to other Service Component Provider(s), DIR, DIR Customers, and authorized Third Party Vendors, which access shall include all appropriate and required licenses and/or interfaces.
2. Limit access to the security clearance database to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.
3. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the security clearance database.
4. The database shall at a minimum should including: full name, company, position/title, manager, physical location, date of clearance, additional agency clearances, agency badges issued, agencies supported, security program training, background checks, privileged access, security badge inventory, access rights, and other rights and controls to physical and logical access.
5. Grant DIR access to the database(s) and allow DIR to monitor and view on an ongoing basis.

A.2.6.4 Physical Security Administration

Service Provider's responsibilities include:

1. Communicate the physical and logical security management processes and procedures to Service Provider and each other Service Component Provider(s) with which an OLA exists.
2. Comply with Service Provider physical and logical security responsibilities.
    2.1. Ensure proper segregation of duties exists where appropriate, including where processes span to Service Provider, other Service Component Provider, and/or Third Party Vendor(s).
    2.2. Notify DIR if it is not possible to maintain the proper segregation of duties.
3. Inform DIR and DIR Customer immediately if Service Provider becomes aware of any vulnerability or weakness in the Services, and recommend a solution or mitigation.
4. Provide reports, on at least a weekly basis, to DIR and DIR Customers to identify those physical access rights that should be removed from DIR and DIR customer locations.

5. Integrate the Physical Security Administration process with Service Management processes, including IT Service Continuity Management.

A.2.6.4.1 DIR and DIR Customer Sites

Where Service Provider uses or visits locations and facilities at DIR and DIR Customer Sites, Service Provider's responsibilities include the following:

1. Ensure compliance with all DIR and DIR Customer security policies, standards and procedures, and all applicable laws and regulations, as they may be revised or updated.

1.1. Comply with DIR and DIR Customers' policies, including security, OHS, data and records management, and electronic records and data archiving.

1.2. Integrate Service Provider's Physical Security Administration process with DIR's, DIR Customers, other Service Component Provider's, and Third Party Vendor(s)' Physical Security Administration processes, where the processes interact.

A.2.6.4.2 Other Locations

Where Service Provider uses other locations and facilities to support the provision of Services to DIR or DIR Customers Service Provider's responsibilities include the following:

1. Provide security processes, facilities, Equipment, and Software that meet or exceed DIR's physical security policies, standards, and procedures. Such processes and physical attributes will be at a minimum consistent with similar security provisions maintained by large, well-managed sourcing services companies.
2. Upon request, provide DIR, its representative(s), and/or regulatory agencies access to all facilities and assets used in providing the Services for audits, investigations, and compliance reviews.
3. Perform all physical security functions (e.g. identification badge controls and alarm responses) at facilities under Service Provider's control.

A.2.6.5 Logical Security Administration

Service Provider's responsibilities include:

1. Establish and maintain mechanisms to safeguard against the unauthorized access, destruction, loss, or alteration of DIR and DIR Customers' data. Service Provider will implement safeguards that are no less rigorous than the practices performed by DIR and DIR Customers as of the Commencement Date.
2. Manage and administer access to Service Provider-operated systems, networks, Software, and DIR and DIR Customers data, to include the following:

   2.1. Upon request provide DIR IT Security full administrative rights related to systems regarding the Services, including full access to audit trails and logs.

   2.2. DIR and DIR Customers will retain authority for approval of all data and system access requirements.

   2.3. DIR and DIR Customers will notify Service Provider regarding the entities and personnel to be granted access to Service Provider-operated systems and the level of security access granted to each.

   2.4. Follow DIR's and DIR Customers' instructions and the procedures regarding such access as designated by DIR or DIR Customers.

2.5. Ensure that the comprehensive database of security clearances and access rights is maintained and tracking all the logical access rights of Service Provider personnel to systems associated with providing the Services.

3. Review all documented information security procedures with DIR pertaining to Service Provider-operated systems.

4. Comply with DIR policies on privacy protection and protective security for data, including security, data and records management, and electronic records and data archiving.

5. Conform to the requirements in accordance with government guidelines and DIR and DIR Customer security policies.

6. Assist in the development, testing and utilization of an action plan and escalation procedures for any potential or real security breaches and report any potential or real security breaches to DIR or DIR Customers per the plan.

7. Monitor users of the systems and Services for authorized access, and monitor, review, and respond and appropriate manner to access violations within designated timeframes.

8. Document and identify security risks associated with the Services, and in support of Risk Management.

9. Notify DIR and DIR Customer in the event of a security violation or unauthorized attempt to access or alter DIR or DIR Customer data, where the notification and escalation is made according to security policy guidelines and procedures.

10. Conduct semi-annual reviews, as appropriate, to validate that individual employee access to programs and libraries is appropriate for Service Provider-operated systems. And provide reports to DIR and DIR Customers.

11. Provide reports, on at least a weekly basis, to identify to DIR and DIR Customers those accounts that should be removed on systems for Service Provider-operated systems.

12. Capture data regarding routine access and exceptions for audit trail purposes, ensure that time stamps are synchronized with a common time source for event correlation and make such data available to DIR or DIR Customers upon request.

13. Perform security audits, provide Incident investigation support, and initiate corrective actions to minimize and prevent security breaches.

14. Provide reports on violation and access attempts, and retain documentation of the investigation.

15. Having obtained DIR approval, install, update, and maintain Software that will provide security monitoring, alarming, and access-tracking functionality for Service Provider-operated systems and Software.

16. Provide security access control tools for data, Software, and networks in compliance with DIR security policies, standards and procedures; and maintain such security and access control devices in proper working order.

17. Develop, implement, and maintain a set of automated and manual processes designed to enforce DIR and DIR Customer’s data access and security policies and procedures.

18. In coordination with DIR IT Security, establish procedures, forms, and approval levels for assigning, resetting, and disabling IDs and passwords used for data or system access by Authorized Users.
    18.1. Execute all related administration for user IDs and passwords.
    18.2. Be responsible for all related administration for user IDs and passwords for Service Provider-operated systems.
    18.3. Regularly review account activity and disable inactive accounts.
19. Communicate with Authorized Users regarding requests for system or data access, and coordinate with DIR and DIR Customer IT Security, which authorizes access to all DIR or DIR Customer data and systems.
20. Run periodic reports to identify accounts that should be removed/disabled or unusual disk space usage of a particular Authorized User or group, and provide reports to DIR IT Security.
21. Coordinate system password changes and, subject to DIR or DIR Customers’ approval, change and test all local passwords as required.
22. Perform backup and recovery procedures in response to security violations that result in lost/damaged information.
23. Respond to all security validation and audit requests from DIR and/or regulatory authorities.
24. Cooperate and assist with efforts by DIR, DIR Customers and/or representatives of DIR for security tests (e.g. validation efforts, audits, Third Party security tests, the annual Control Penetration Test).
25. Work together with DIR to change security in responses to evolving requirements and changing technology and related processes.
26. Establish and maintain safeguards against the unauthorized access, destruction, loss, or alteration of DIR or DIR Customer data in the possession of Service Provider, where the safeguards are at least as stringent as DIR policies.
27. Integrate Service Provider’s Logical Security Administration process with DIR’s, DIR Customers, other Service Component Provider's, and Third Party Vendor(s)’ Logical Security Administration processes, where the processes interact.

A.2.6.6 Risk Management

Service Provider is charged with providing Risk Management related to the IT environment and Services within the context of the organization's overall business risks. The goal of Risk Management is to quantify the impact to the business that a loss of service or asset would have, to determine the likelihood of a threat or vulnerability to actually occur, and then to manage activity against the identified risks.

Service Provider’s responsibilities include:

1. Establish on-going activities, including supporting processes, for the identification, analysis, quantification and management of risks in the IT environment, in support of DIR and DIR Customer business risk management.

2. Establish and maintain a Risk Register as an on-going log of identified risks and corresponding counter measures, that at a minimum will contain:
   2.1. Scope of risk, including the effected DIR Customer and particular assets.
   2.2. Owners of risk who will be responsible for risk mitigation activities as required.
   2.3. Priority of each risk.
   2.4. Status of each risk.
   2.5. Severity of each risk in terms of information, value, or legality.
   2.6. Decisions by DIR and DIR Customers as to measures and mitigations for each risk.
   2.7. Any other supporting information or associated policy, code or requirements.
3. Review the Risk Register with DIR and DIR Customers on a regular basis, and provide recommendations for mitigation or disposition.
4. Collect and assess risks from multiple areas and disciplines, including but not limited to:
   4.1. Risks associated with policy deviations and audit findings.
   4.2. Risks associated with Business Continuity test results and Disaster Recover test results.
   4.3. Risks associated with long-term programs and their managing plans (e.g. Refresh, Transformation and Consolidation, IT Service Continuity and Disaster Recover).
5. Provide Risk Management input to other programs toward the long-term reduction of risk in the environment (e.g. Capacity Plan, Long-Range IT Plan, Refresh Plan, and Transformation Plans).
6. Provide an overall Risk Management Plan for reducing risk in the IT environment, and report to DIR on at least an annual basis.
   6.1. Support the Risk Management planning activities of DIR and DIR Customers in regards to the Services and IT environment, and in compliance with TAC 202.

A.2.7 Vendor Management and Coordination

Service Provider’s responsibilities include:

1. Manage and coordinate the activities of all Service Provider Third Party Vendors (e.g. Server connectivity, facility manager, auditors, security service provider, broadband provider, wiring contractors).
2. Maintain technical support relationships with Service Provider Third Party Vendors to resolve Incidents and Problems with the Services and to provide answers to technical questions and requirements related to the use of the Third Party Vendor’s products or services.

A.2.7.1 Service Component Management and Coordination

Service Provider’s responsibilities include:

1. Create, manage and maintain OLAs with all Service Component Providers in regards to the Services.

2. Manage Service Component Providers service delivery in compliance with OLAs.

3. Monitor other Service Component Provider service delivery and performance in regard to the Services, including:

   3.1. Monitor the other Service Component Provider's compliance with any service levels contained in any agreement between DIR and the other Service Component Provider.

   3.2. Provide integrated compliance reporting for the monitoring and management of service levels contained in any agreement between DIR and the other Service Component Provider when the other Service Component Provider is contractually required to provide compliance reporting data in a mechanized format.

   3.3. Maintain consistent use of reporting standards, formats, and so forth across Service Provider and the other Service Component Provider.

   3.4. Notify DIR and the other Service Component Provider of each other Service Component Provider failure to perform in accordance with the provisions of its agreement.

   3.5. Evaluate and recommend retention, modification, or termination of Service Component Providers based on the performance or cost benefits to DIR as tracked by Service Provider.

A.3 Equipment and Software Services

A.3.1 Long Range Planning

Service Provider will provide a process for the establishment, currency, tracking, and publishing of a Technology Plan that incorporates input from DIR, DIR Customer and DCS Service Providers and aligns with the Governance processes set forth in **Exhibit 6**. Service Provider's responsibilities include the following:

1. Develop and update the long-range, comprehensive plan for DIR's and DIR Customers information technology (IT) systems, processes, technical architecture and standards (the "Technology Plan").
    1.1. DIR and DIR Customers shall approve the plan, in conjunction with IT Governance as described in **Exhibit 6**.
    1.2. The Technology Plan will be developed on an annual basis, and will include a rolling three (3) year projection of anticipated changes (subject to DIR business and planning requirements).
    1.3. Coordinate the aggregation of technical planning information from DIR, DIR Customers, Service Provider, other Service Component Providers, and other Third Party Vendors as directed by DIR.
    1.4. Provide an implementation road map with estimated timing and cost impacts, in a format consistent with Charges, for DIR and DIR Customers.
    1.5. Provide linkage with technology currency requirements that align with technology refresh plans (e.g. software version migrations).
2. Help to understand, develop, and confirm the future business and IT requirements.
3. Assist in projecting future volume, technology, and geographic changes that could impact DIR's and DIR Customers systems and technical architectures.
4. Identify candidates and requirements for the deployment of new technology or the automation of tasks associated with the Services and/or DIR's and DIR Customers business processes.
5. Proactively submit proposals regarding new technology and automation to DIR for its review and approval.
6. Proactively seek to automate manual tasks associated with the Services.
7. Support DIR and DIR Customers in the proposal and presentation of changes in technology product and service offerings.
8. Facilitate and encourage active cross-functional, cross-group, and cross-location coordination and communication related to technology changes and automation.
9. Proactively identify strategies and approaches for future IT delivery that Service Provider believes will provide DIR and DIR Customers with competitive advantages and that may result in increased efficiency, performance, or cost savings.
10. As part of each annual planning cycle, provide specific, short-term steps and schedules for projects or changes expected to occur within the first twelve (12) months of each plan.

11. Help to specify the Equipment and Software architecture and standards, and participate in continuously keeping DIR's and DIR Customers' technical architectures current.
12. Facilitate appropriate access to specialists within Service Provider's other organizations, as needed, to assist DIR and DIR Customers in developing and updating the plans.
13. Identify industry and technological trends that may impact DIR's and DIR Customers' plans.
14. Help identify and track regulatory issues/changes that may impact DIR's plan.
15. Gather and incorporate the data and lessons learned from the operating environment that may impact DIR's and DIR Customers' plans.
16. Perform trend analysis from the resource consumption data to project future demand that may impact DIR's and DIR Customers' plans.
17. Cooperate with DIR and DIR Customers in researching and implementing automated tools to improve Service Levels and/or performance of the computing environment. Tool selection will be in accordance with DIR and DIR Customers' standards and technical architectures.

A.3.2 Evaluation and Testing

Service Provider's responsibilities include the following:

1. Ensure that DCS Service Providers have established effective Evaluation and Testing procedures and plans to meet DIR Customer performance requirements.
2. Ensure that procedures for Evaluation and Testing are properly documented in the Service Management Manual.
3. Monitor and report on DCS Service Provider evaluation and testing of Equipment, Software, and related products and services.

A.3.3 Refresh and Technical Currency

Service Provider's responsibilities include the following:

1. Refresh as required in **Attachment 4-B** throughout the Term, for purposes that include meeting DIR's and DIR Customers' business requirements; preventing technological obsolescence or failure; and accommodating volume changes, the ability to increase efficiency, the ability to lower costs, and/or the need to maintain the required Third Party Vendor support.
2. Establish an on-going Refresh Program that accomplishes the Refresh goals and coordinates the activities of DIR, DIR Customers, other Service Component Providers and designated Third Party Vendors, at the direction of the DIR.
3. Deploy Equipment and Software associated with any Refresh in accordance with the standards of DIR's technical architecture and the Technology Plan.
4. Accommodate the timeframes and other requirements associated with Refresh, as well as the financial responsibility for the underlying assets, as provided in **Attachment 4-B**.
   4.1. DIR reserves the right to modify the Refresh timeframes and requirements during the Term based on its business requirements, subject to the Change Control procedures.

A.3.3.1 Refresh Responsibility

Service Provider’s responsibilities include the following:

1. Coordinate, monitor and manage the execution of Refresh Responsibilities by DCS Service Providers and designated Third Parties.

A.3.3.2 Software Currency and Release Levels

Service Provider’s responsibilities include the following:

1. Monitor “end-of-life” hardware and software processes resident in each DCS Service Provider’s technology plan and ensure proper notification is provided to DIR, DIR Customer and Third Party Vendors regarding support and software currency plans.
2. Unless otherwise directed by DIR, provide and support Software under Service Provider’s operational responsibility at the most recently released and generally available version of the Software (the “N” release level).
3. As directed by DIR, also support release N-1 and earlier versions of the Software for the longer of the following:
    - 3.1. The thirty-six (36) month period following version N’s general public availability.
    - 3.2. The time the Third Party Vendor ceases to support such version.
4. Use commercially reasonable efforts to support Software that is no longer supported by the Third Party Vendor.
5. Provide support for all Software versions and release levels that exist as of the Effective Date until otherwise directed by DIR.
6. Provide monthly reports of upcoming software releases, software renewals and end-of-support notices to DIR and affected DIR Customers, at least 180 days prior to expirations date.

A.3.3.3 Refresh Planning

Service Provider’s responsibilities include the following:

1. In coordination with DIR, DIR Customers and DCS Service Providers develop and manage a continual plan for Refresh, including:
    - 1.1. Within one-hundred and twenty (120) days prior to DIR’s annual planning process meetings, review the asset inventory and produce a report that lists the assets that are due to be refreshed in the upcoming plan year, and provide such report to DIR’s annual planning process.
    - 1.2. Coordinate planning activities with DIR, DIR Customer, other Service Component Providers and designated Third Party Vendors.
    - 1.3. Service Provider and DIR will consider the usability of the assets and review alternatives to replace, re-lease, consolidate, or retain the assets. Based on the results of this review, Service Provider will deliver the initial recommendations regarding such assets to DIR within thirty (30) days after the review.

1.4. For Service Provider-owned assets, Service Provider and DIR will mutually determine whether Service Provider will replace an asset and the appropriate replacement date.

1.4.1. If Software Changes are required due to replacement of assets, Service Provider, in consultation with the DIR, will review alternatives for making changes to such Software.

1.4.2. Such replacement of the assets and Software will be at Service Provider's expense if the replacement is required to facilitate achievement of the agreed upon Service Levels or because the asset is obsolete (i.e. replacement parts cannot be acquired or the asset has become unserviceable).

1.5. For DIR and DIR Customer owned and leased assets, based on the planning process outcome and direction established by DIR, Service Provider will provide a proposal for refresh of those assets (replacement at DIR's expense) to DIR.

2. Adhere to DIR's approved plan, and execute that plan utilizing established procurement processes, to initiate refresh and retirement activities.

2.1. Provide monthly reports 180 days prior to lease expiration date showing assets to be refreshed with latest data.

2.2. Notify DIR monthly of all open agreements related to assets that are retired or will retire within 180 days of the report date.

3. Track and report on the completion progress of asset Refresh.

4. Update and archive asset records after retirement.

A.3.4 Service Catalog

Service Provider's responsibilities include the following:

1. Provide the format, repository and access capabilities for all DCS Services in an enterprise Service Catalog.
2. Coordinate all updates to the Service Catalog with Service Providers and DIR.
3. Create and regularly (at least every ninety (90) days) update a list of Equipment and Software that includes the approved products for purchase or lease by Authorized Users (the "Service Catalog").
4. Align the Service Catalog contents with DIR's strategic direction, technical architecture, refresh strategy, and product evaluation and test results. DIR will retain approval for the Service Catalog contents.
5. Maintain the Service Catalog on a relational database system, which contains links/integration with the Asset Inventory and Management System as necessary and appropriate. DIR will retain approval for the database design and will have access to the database.
6. Cooperatively provide access to the Service Catalog for specific Third Party Vendors to list and maintain their Equipment, Software, Services and other Products, as directed by DIR. Such access must include the capability to mechanize and automate the maintenance.

A.3.4.1 Service Catalog Contents

Service Provider's responsibilities include the following:

1. Categorize the Service Catalog contents by type of service, configuration type, and/or Equipment or Software type (e.g. IMACS, network, printers, etc.).
2. Include individual services, Equipment and Software items, as well as entire configurations of Services, Equipment and Software, as applicable, based on the deployment standards or options (e.g. DNS change, asset move, site information change, DIR Customer account code change, remote VPN service, Portal access, SP tool access, user provisioning, Oracle license.).
3. Where DIR and DIR Customers are financially responsible for Equipment and Software contained in the Service Catalog, the Service Catalog should contain the preferred financing approach (purchase or lease) as determined by DIR.
   - 3.1. If the preferred approach is to purchase, the list will contain the current purchase amount.
   - 3.2. If the preferred approach is to lease, the list will contain the current monthly lease amount and the lease term.
   - 3.3. If the preferred approach is to lease, the list will provide a mechanism for direct purchase to support alternate sources of funding (e.g. grants).
4. Include any notation required for specific use (or limitation) of the Equipment or Software – or of the delivery of the service – by region, by business unit, or by category of Authorized User.
5. Include any technical limitations/requirements for the use of Equipment or Software (e.g. minimum disk space, memory, operating system etc.) or execution/delivery of the service.
6. Indicate the approval authority required to obtain the service, Equipment, or Software.
7. Include a description of how to obtain additional information about the service, Equipment, or Software.

A.3.4.2 Service Catalog Distribution

Service Provider's responsibilities include the following:

1. Create and distribute regular communications with DIR and DIR Customers on updates to the Service Catalog, as approved by DIR.
2. Publish and make available the Service Catalog to Authorized Users as requested by DIR.
3. Make the Service Catalog available through the Portal, along with search capabilities and contact information for queries.

A.3.5 Standard Products

Service Provider's responsibilities include the following:

1. Create and regularly (at least every ninety (90) days) update a description of minimum Equipment and Software requirements and specific Equipment and Software that are designated for standard use within DIR (the "Standard Products").

1.1. Publish and make available the description of Standard Products to Authorized Users as requested by DIR.

1.2. Make the description of Standard Products available on the Portal.

1.3. Provide search capabilities and contact information for queries.

2. Align the Standard Product list with DIR's strategic direction, technical architecture, and refresh strategy.

3. Provide mechanisms and processes and procedures to capture feedback and business needs from DIR Customers as to changes in Standard Products.

4. Maintain the Standard Products list on a relational database system, containing links and integration with the Asset Inventory and Management System as necessary and appropriate.

4.1. Database design is approved by DIR.

4.2. Grant access to DIR to the database.

A.3.5.1 Standard Product Descriptions

Service Provider's responsibilities include the following:

1. Focus on broad, minimum requirements rather than on specific models or configurations (e.g. minimum processor type, minimum release level of Software, etc.).
2. Emphasize standards that are easily understood by Authorized Users.
3. Include internally-developed Software that is approved for use by DIR and DIR Customers.
4. Identify differences between geographic regions, business units, or type of Authorized User, based on DIR and DIR Customers' business requirements.
5. All Equipment and Software included in the Service Catalog are considered to be Standard Products.
6. All Equipment and/or Software in use, which is within the refresh cycle approved by DIR and which may be changed from time to time based on technological change and/or business requirements, will be considered to be Standard Products.
7. All Equipment and Software in use as of the Commencement Date will be treated as Standard Products for a minimum of twenty-four (24) months after the Commencement Date and will not be treated as out of compliance until after the 24 month period or as determined by the appropriate governance committee.
8. Changes to Standard Products are approved by the appropriate governance structure in accordance with **Exhibit 6**.

A.3.5.2 Standard Products Monitoring and Reporting

Service Provider's responsibilities include the following:

1. Routinely educate DIR Customers about the need and requirements to use Standard Products, including bulletins about upgrade requirements, modification of product support, compatibility issues, known problems with nonstandard products, etc.

2. Monitor the environment for the introduction and use of nonstandard products within DIR.
3. Where an Authorized User is not utilizing a Standard Product, take proactive steps to inform the Authorized User and include steps the Authorized User should take to obtain a Standard Product or to replace the one currently in use.
4. Use and update the Asset Inventory and Management System to determine the potential use of nonstandard Equipment and/or Software by an Authorized User.
5. On at least a monthly basis, provide a report to DIR that lists all users that are not using Standard Products, and include the specific use of the nonstandard Equipment and/or Software.
6. Provide information to Authorized Users who will be affected by the elimination of a Standard Product at least twelve (12) months prior to the elimination of a Standard Product from the list. This communication to Authorized Users will include the following:
   - 6.1. Transmit the information via a broadcast email or post it on the Portal, subject to approval by DIR.
   - 6.2. Provide information regarding the future minimum Standard Product and/or the item in the Service Catalog that should be used as a replacement.
   - 6.3. Provide information regarding who to contact or where to obtain additional information about the change to the Standard Product list.

A.3.6 Delivery and Staging

Service Provider is responsible for the coordination of, tracking and escalation necessary to ensure DCS Service Providers meet commitments related to Delivery and Staging of Equipment and Software to meet scheduled project commitments to DIR Customer.

A.3.7 Equipment and Software Maintenance

Specific operational responsibilities for various categories of Software are described in the Statement of Work, and in **Attachment 4-B**.

Where Service Provider is financially responsible for the underlying Equipment or Software, Service Provider’s responsibilities include the following:

1. Coordinate and manage all Third Parties that provide maintenance-related support for Equipment and Software used in conjunction with the Services.
2. Perform all maintenance of Equipment and Software in accordance with Change Management procedures, and schedule this maintenance to minimize disruption to DIR’s and DIR Customers’ business.
3. Provide or arrange for qualified Third Parties to provide maintenance for such Equipment and Software.
4. Provide such maintenance as necessary to keep the assets in good operating condition and in accordance with the manufacturer’s specifications, or other agreements as applicable, so that such assets will qualify for the manufacturer’s standard maintenance plan upon sale or return to a lessor.

5. At all times, provide maintenance for Equipment and Software as necessary to meet specified Service Levels, including:

   5.1. Providing maintenance for Equipment and Software not under maintenance contracts.

   5.2. Provider commercially reasonable efforts to maintain Equipment and Software no longer supported by the OEM.

6. For Third Party maintenance contracts, Service Provider responsibilities include the following:

   6.1. Administer and manage the contract on behalf of DIR.

   6.2. Notify DIR in advance about maintenance contracts that are about to expire.

   6.3. Recommend modifications to the services during Third Party maintenance contract renewal.

A.3.8 Software Support

Specific operational responsibilities for various categories of Software are described in the Statement of Work, and in **Attachment 4-B**.

A.3.8.1 Installation, Upgrades and Changes

Service Provider’s responsibilities include the following:

1. Install, upgrade, and change all Software as required and in accordance with DIR technical architecture standards.
2. Interface with DIR, DIR Customer staff and other Third Parties to promote the compatibility of Software products.
3. Unless otherwise directed by DIR, install, upgrade, and change Software to prescribed release levels. (Software Currency and Release Levels are described in Section A.3.3 of this **Exhibit 2.1**.)
4. Provide installation of department or Authorized User-specific Software as requested by DIR and DIR Customers.
5. Install Third Party-supplied corrections for Third Party Software problems, which include installation of Third Party-supplied Software patches as required.
6. Give written notice to DIR at least ninety (90) days in advance of all upgrades and Software changes that are planned to occur in the following calendar quarter. The Parties will mutually agree in writing on the timing for the implementation of upgrades.
7. Coordinate testing, installation, customization, and support of Software with Application Development and Maintenance (ADM) personnel, Authorized Users, and other Third Parties as required.
8. Coordinate with DIR, DIR Customers and DCS Service Providers in the establishment of designated patching windows.
9. Observe DIR Change Management procedures while implementing changes, upgrades, or enhancements.

10. For any changes, upgrades, or enhancements, advise DIR and DIR Customers of any additional Equipment, network, environmental, or other requirements needed during integration testing and/or otherwise known to be necessary for the implementation.
11. Proactively provide ADM staff, DIR, and other Third Parties with support for Equipment and System Software used to support ADM activities.
12. Provide reports, at least monthly, on software upgrades applied, including patching to DIR and DIR Customer.
13. Provide monthly reports of upcoming software releases, software renewals and end-of-support notices to DIR and affected DIR Customers, at least 180 days prior to expirations date.

A.3.8.2 Software Support

Service Provider responsibilities include the following:

1. Maintain documentation on Software that reflects the complexity and diversity of the environment and that enhances the Software support process (e.g. installation, maintenance, interfaces, active processes).
2. Maintain a library of documentation that identifies the Software required to support the Services and the operational support procedures associated with the Software.
   2.1. Maintain, update and ensure currency in the Configuration Management process for all software.
3. Support all Software, excluding Applications supported by DIR’s and DIR Customers’ staff or other Third Parties, as required and in accordance with DIR’s and DIR Customers’ technical architecture standards.
4. Support Software at prescribed release levels or as directed by DIR. (Software Currency and Release Levels are described in Section A.3.3 of this **Exhibit 2.1**.)
5. Correct/make changes to Software as required.
6. Provide Authorized Users with Software support, advice, and assistance.
7. Review all Software conversion, migration, and upgrade plans with, DIR and DIR Customer.

A.3.8.3 Malicious code or unauthorized code Protection

Service Provider’s responsibilities include the following:

1. Install, update, operate, and maintain malware protection or unauthorized code protection Software on all Equipment used to deliver or support the Services (e.g. servers, laptops) in compliance with **Exhibit 17**, TAC 202 and applicable Federal policies.
2. Maintain subscription to the anti-malicious code or unauthorized code Software support in order to proactively receive malicious code or unauthorized code engine and pattern updates.
3. Install updates, in accordance with Change Management, to malicious-protection Software as needed or as directed by DIR or DIR Customer, no later than twenty-four (24) hours after such updates are made available to Service Provider (or qualified Third Parties selected by Service Provider) and approved by DIR.

4. Perform scans for malicious code or unauthorized code on all emails, including email attachments.

5. Upon detection of malware or unauthorized code, take immediate steps to notify DIR, DIR Customer and the Service Desk in compliance with guidelines contained in **Exhibit 17** and the Service Management Manual, as well as to:

    5.1. Assess the scope of damage.

    5.2. Arrest the spread and progressive damage from malware or unauthorized code.

    5.3. Eradicate malware or unauthorized code.

    5.4. Restore all data and Software to its original state.

6. Monitor and scan diskettes or hard drives or other temporary storage devices (such as USB memory sticks, PCMCIA flashcards, FireWire hard drives, etc.) for malware or unauthorized code upon demand.

7. Develop any plans necessary to provide malware protection or unauthorized code protection.

8. Provide consulting services for malware protection or unauthorized code protection.

9. Respond to malware or unauthorized code Incidents.

10. Provide proactive alerts to Authorized Users relative to current malware or unauthorized code threats either specific to DIR’s environment, encountered in Service Provider’s environment, or based on industry information.

11. Provide additional temporary resources in the event of a major computer malware or unauthorized code outbreak so DIR’s and DIR Customers’ performance does not degrade because of an unavailability of Service Provider resources.

12. Provide daily and monthly reports, broken out by DIR Customer and in compliance with DIR and DIR Customer policies that contain a summary of the number of malware or unauthorized code detected and cleaned, as well as a list of malware caught.

A.3.8.4 Intrusion Systems

Service Provider’s responsibilities include the following:

1. Establish processes and procedures in the Service Management Manual with DIR, DCS Service Providers and other designated Third Parties for the management, monitoring, alerting, notifying and reporting of Intrusion Systems.

2. Monitor all intrusion systems from a central logging system, and provide appropriate response to alerts, 24 x 7 x 365, based upon mutually agreed procedures.

3. Review intrusion systems logs and provide appropriate response to messages including, but not limited to, alerts and access denial messages, based upon mutually agreed procedures.

4. Provide alerts to DIR and DIR Customers relative to current intrusion threats either specific to DIR’s and DIR Customers environment, encountered in Service Provider’ environments, or based upon industry information.

5. Upon detection of an intrusion alert, take immediate steps to notify DIR, DIR Customer, and the Service Desk in compliance with guidelines contained in **Exhibit 17** and the Service Management Manual and to:

    5.1. Assess the scope of damage.

    5.2. Arrest the spread and progressive damage from the intrusion.

    5.3. Restore the environment to an operational state.

    5.4. In the event of corruption or data loss, restore data from the last available backup.

6. Evaluate technology improvements for intrusion and bring forth those improvements to DIR for consideration.

A.3.9 Administration

A.3.9.1 Asset Inventory and Management

Service Provider's responsibilities include the following:

1. Provide and maintain an Asset and Inventory Management System (AIMS) that can track and manage all Equipment, Software, and related services (e.g. circuits).

    1.1. Provide access to the AIMS to other Service Component Provider(s), DIR, DIR Customers, and Authorized Third Party Vendors, which access shall include all appropriate and required licenses and/ interfaces.

2. Develop and implement policies and procedures, with DIR approval, for schema, taxonomies, asset and inventory information, and general guidelines for asset and inventory management.

3. Integrate the AIMS with other systems for Service Management, including Configuration Management, Change Management, and Release Management.

    3.1. Integrate the associated AIMS database with the Asset and Inventory Management Databases of other Service Component Provider(s), and designated Third Party Vendor(s), as directed by DIR.

4. Limit access to the AIMS to the agreed levels (e.g. by DIR Customer) for the type of Authorized Users who require access to the systems.

5. Provide Service Provider personnel, other Service Component Provider(s) personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the AIMS.

6. Grant DIR access to the database(s) of the AIMS, and allow DIR to monitor and view on an ongoing basis.

7. Provide for and manage the tracking and renewal of software licenses to ensure compliance with agreements and continued operation in the environment.

8. Manage and conduct an initial, complete inventory of all Equipment, Software, and related services provided or supported by Service Provider and deployed at DIR and DIR Customers Sites or Service Provider locations. This initial inventory will include all IT assets, whether such assets are owned or leased by DIR, DIR Customers, or Service Provider.

9. Schedule and manage to completion this initial inventory in accordance with the Critical Deliverables as listed in **Attachment 3-C**.

10. Record, at a minimum, the individual data elements for each asset as part of the initial inventory as specified in **Attachment 6-B** and as applicable for individual asset types.

11. As the initial asset inventory is being conducted, enter the required information regarding the assets into Service Provider's AIMS.

    11.1. DIR will approve the AIMS and the initial inventory before final implementation.

12. Produce periodic reports as necessary, and respond within designated timeframes to queries and requests concerning the inventory data or supporting information. At a minimum, such reports shall include:

    12.1. Exception reports on errors and corrections, by DIR Customer.

    12.2. Reports on the results of periodic validations and inventories.

13. Develop, implement, and maintain automated asset management tools for all Services and Service Provider-provided processes that:

    13.1. Support auto discovery.

    13.2. Facilitate effective deployment and re-use of DIR, DIR Customers and Service Provider-owned technology assets.

    13.3. Enable a common view in terms of information access and presentation by DIR, DIR Customers and Service Provider.

14. On a periodic basis (at least every six months), electronically validate all asset data in the AIMS

15.

16. Ensure DCS Service Providers policies and procedures include processes to verify inventory information upon an Authorized User's request for on-site service.

17. Continuously update the AIMS, and at the minimum accomplish the following:

    17.1. Remove assets that are no longer in use, in accordance with DIR policies.

    17.2. Modify asset information resulting from asset relocation and/or use by a different Authorized User.

    17.3. Modify asset information due to upgrades and Software updates.

    17.4. Add new asset information upon implementation of new Equipment or Software.

18. Manage the annual logical inventory on all DIR and DIR Customer owned assets that are part of Services.

    18.1. Perform all validation and reconciliation activities associated with inventory, including updates to the CMDB.

19. Maintain a secure Definitive Media Library, which holds the logical index to all definitive media (including software and associated documentation) and in accordance with the Release Management section of **Attachment 6-B** for all Software, except those versions of DIR and DIR Customers' custom developed Application Software released

into the development and test environments (i.e. not released into the production environment).

20. Maintain a secure logical index that stores the locations of definitive hardware spares and maintains them at the same level as the live location, including recording their details in the CMS / CMDB.
21. Where Equipment has been identified by DIR and DIR Customer as exempt or as co-located, Service Provider will track those items and ensure they are exempted from receipt of the applicable Services.

A.3.9.2 License Management and Compliance

Service Provider's responsibilities include the following:

1. Manage compliance with all Software licenses by validating all Software use, regardless of financial responsibility for the Software (e.g. security, certificates).
2. Proactively manage the use of the Software in order to maintain strict compliance, including:
   - 2.1. Immediately notify and advise DIR of all Software license compliance issues associated with the Services and DIR-retained Software.
   - 2.2. For DIR-retained Software, track and maintain the applicable licensing and use information received from DIR Customers.
   - 2.3. Report on Equipment with the presence of any unauthorized or non-standard Software.
   - 2.4. Track license counts and associations within the CMDB.
   - 2.5. Manage and track security certificates used to secure confidential sessions (e.g. SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals, as required by DIR or DIR Customers.
3. Confirm the presence and version of Software installed on a particular device and that those attributes are recorded in the asset management system.
4. Provide reporting of license information and compliance to DIR, at least quarterly or as directed by DIR.

A.3.9.2.1 Service Provider License Management and Compliance

Where Service Provider is financially responsible for Software associated with the Services, Service Provider's responsibilities include the following:

1. Manage compliance with all Software licenses by monitoring and validating Software use.
2. Proactively monitor the use of the Software in order to maintain strict compliance, including:
   - 2.1. Immediately notify and advise DIR of all Software license compliance issues.
   - 2.2. Provide the Software and acquire the correct number of the licenses to be compliant with Service Provider's Third Party Vendor requirements.
   - 2.3. Monitor the Equipment for the presence of any unauthorized or non-standard Software.

2.4. Track license counts and associations.

2.5. Manage and track security certificates used to secure confidential sessions (e.g. SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals.

3. To the extent enabled by Service Provider-provided and DIR-approved enterprise management system, perform the following activities:

3.1. Define and check for particular Software signatures.

3.2. Monitor the use of Software developed by Service Provider application development groups.

3.3. Check the presence and version of Software installed on a particular device and record in the asset management system.

3.4. Provide reporting of license information and compliance to DIR, at least quarterly or as directed by DIR.

3.5. File and track Software license agreements and associated license keys, including processes and procedures for renewals; associate with CI in the CMDB.

A.3.9.3 Effective Use of Equipment and Software

Service Provider's responsibilities include the following:

1. Proactively identify strategies and approaches that will result in the elimination of unnecessary Equipment or Software, or modifications to existing Equipment and Software that Service Provider believes will provide DIR and DIR Customers with competitive advantages, increased efficiency, increased performance, or cost savings.
2. On a semi-annual basis, formally identify and review with DIR and DIR Customers the efficiency opportunities that Service Provider has observed during the course of providing the Services, and review changes that have already been made with the approval of DIR and DIR Customers, regardless of financial responsibility for underlying assets.
3. Provide processes and procedures for effective re-use and re-deployment of assets (e.g. Equipment and Software) including use in Solution Requests.
4. Track the availability to reuse and re-deploy assets, in compliance with DIR and DIR Customer policies.

A.3.9.4 Site Information Management

Service Provider's responsibilities include the following:

1. Manage the inventory of all locations receiving Services and designated by DIR, and validate the Site Information in **Exhibit 7**.
2. Maintain a comprehensive and master listing of DIR and DIR Customer Sites receiving Services.

2.1. Provide access to the master list to DIR, DIR Customer, Service Providers, and designated Third Parties.

3. Provide for and maintain meaningful cross-references to site nomenclature and identifiers within DIR, DIR Customer and Third Party Vendor systems as specified by DIR.
4. Ensure that Site Information is accurately maintained and distributed to support the delivery of Services, and in a manner consistent with all of Configuration Management.
5. Ensure that all Service Provider tools, systems, databases, FAQs, documents, training material and other relevant areas are regularly updated with Site Information.
6. Provide tools, processes, and procedures for DIR and DIR Customers to request changes to the Site Information. Document and maintain processes within the Service Management Manual and in appropriate Third Party Vendor processes and procedures.
7. Provide updates based on DIR and DIR Customer change requests within designated timeframes.
8. Regularly provide complete Site Information to DIR, DIR Customer and authorized Third Parties as specified by DIR.
9. Document and escalate to DIR where other key partners, Service Providers and relevant Third Parties are not accurately or updating Site Information within designated timeframes.

A.3.10 Redeployment and Disposal of Equipment

Service Provider’s responsibilities include the following:

1. Establish processes and procedures for the re-use and redeployment, in compliance with DIR policies and document in the Service Management Manual.
    - 1.1. Upon redeployment or disposal of Equipment, ensure that necessary changes are made in the Asset Inventory and Management System.
    - 1.2. Track the availability of re-usable assets in the CMS/CMDB as an index to the available hardware spares.
    - 1.3. Consider the available assets and Equipment for fulfilling Service Requests and Requests for Solutions.
2. Prior to a new purchase or lease of any Equipment, advise DIR or DIR Customers of any possibility of re-deploying existing Equipment.
3. Verify and track that unusable Equipment has been surplused per policies and procedures set out in the Service Management Manual.

A.4 Other Services

A.4.1 Project Management and Support

Project Management and Support will align projects to DIR and DIR Customer requirements and deliver projects from request through end to end solution including turnover to the DIR Customer and validation that project requirements were met in terms of timing, quality, and cost.

Service Provider's responsibilities include:

1. Facilitate and lead in the development and documentation of processes with Service Provider and other Service Component Provider(s).
2. Facilitate and lead information exchange between and among Service Provider and other Service Component Provider(s), DIR and DIR Customer, and/or Third Party Vendor(s) to improve Project Management.
3. Validate that the Project Management process provides an audit trail that meets the legislative and policy requirements to which DIR and DIR Customer must comply.
4. Integrate Service Provider's Project Management process with the Project Management processes of other Service Component Provider(s), DIR and authorized Third Party Vendors, with and where the processes interact.
5. Integrate Service Provider's Project Management process with the other Service Management processes, including Request Management and Fulfillment, Release Management, Change Management, Configuration Management and IT Financial Management.
6. Coordinate Project Management activities across all functions, other Service Component Provider(s), DIR Customer Sites, regions, and Third Party Vendor(s) that provide services to DIR Customer.
7. Conduct regularly scheduled Project Management meetings.
    - 7.1. Document and publish Project Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other Service Component Provider(s) and authorized Third Party Vendors.
8. Communicate and coordinate the Project Management Process within Service Provider's own organization, other Service Component Provider(s), DIR, DIR Customers, and designated Third Party Vendor(s).
    - 8.1. Provide on-going methods for training Service Provider staff, other Service Component Provider(s), DIR, DIR Customers and designated Third Party Vendors on the Project Management processes.
9. Facilitate and lead in the definition and documentation of Project Management Policies, as approved by DIR, which set the objectives, scope and principles that will ensure the success of the Project Management processes.
    - 9.1. Continually verify the effective compliance with the Project Management Policies by Service Provider, other Service Component Provider(s), and designated Third Party Vendors.

10. Establish on-going Project Planning activities with DIR and DIR Customers in coordination with other Service Component Provider(s) and designated Third Party Vendors.
11. Establish a single focal point for Project considerations and issues in order to minimize the probability of conflicting priorities.
12. Establish processes for forecasting DIR and DIR project requirements and in coordination with other DCS Service Provider(s) and designated Third Party Vendors.
13. Lead demand management activities to encourage Authorized Users to make the most effective use of Service Provider resources and to assist DIR to minimize its costs while maximizing the value it receives from the Services.

A.4.1.1 Project Planning

Service Provider's responsibilities include the following:

1. Maintain appropriate levels of industry knowledge in DIR's business in order to provide support and recommendation of projects. The knowledge will be obtained and maintained through, among other activities, participation in industry meetings, forums, and conferences at Service Provider expense.
2. Coordinate the preparation of proposals and plans for projects as requested by DIR and DIR Customers or as appropriate based on providing the Services. Such proposals and plans will be provided to DIR and DIR Customers in a consistent structure/format and include:
   - 2.1. Develop and utilize a set of project proposal models to establish consistency in format and content detail.
   - 2.2. The business requirements for the work and the deliverable(s) desired.
   - 2.3. The functional and/or technical approach and solution.
   - 2.4. The initiator of the proposed project (either an Authorized User or Service Provider).
   - 2.5. The total number and type(s) of FTEs required for the project.
   - 2.6. A description of any Equipment, Software, or other materials required for the project and ongoing support.
   - 2.7. The total elapsed time to complete the project, and any time constraints or material assumptions.
   - 2.8. The total cost of the project (including fees paid to Service Provider as well as any Retained Expenses), the timing of any payment(s), and whether the cost is included in the Base Charges.
   - 2.9. The ongoing annual cost of the project post-implementation (including fees paid to Service Provider as well as any Retained Expenses and Pass-Through Charges), the timing of any payment(s), and whether the cost is included in the Base Charges.
   - 2.10. Any other material assumptions, including but not limited to risks, mitigation plans, dependencies, costs and/or any other item related to the project, including any support required from DIR and DIR Customers or its Third Party Vendor(s).

2.11. Any other provisions necessary to describe the work needed.

3. Coordinate proposal creation with other DCS Service Providers and designated Third Parties, in conjunction with Request for Solution processes.

4. After DIR and DIR Customers approve a project related to the Services, employ a Project Management methodology that will be used as a tool to consistently plan, initiate, control, and implement all projects for all Services.

4.1. Coordinate and negotiate a target project completion date with DIR Customers and other Third Party involved in delivery of the project.

4.2. Provide project managers with experience in the methodology and a proven track record of success in using it to manage projects.

4.3. Coordinate with DIR to gain approval for use of the methodology prior to deployment.

5. Provide DIR, DIR Customers with a profile of project work and each projects current status on a monthly basis or as requested.

A.4.1.2 Current and Ongoing Projects

A list of the major Current and Ongoing Projects are set forth in **Exhibit 9**.

As of the Commencement Date, DIR will have the right to update the projects listed in **Exhibit 9** to include any additions to and deletions from such list, which have occurred in the ordinary course of business prior to the Effective Date.

Service Provider’s responsibilities include

1. If requested by DIR or DIR Customers, complete all Ongoing Projects in accordance with the following:

1.1. Complete all Ongoing Projects in accordance with project management and development practices in place as of the Effective Date, unless modified by mutual consent.

1.2. Use all commercially reasonable efforts to complete the Ongoing Projects in compliance with **Section 4.7** of the Agreement.

1.3. Use the project change management procedures to address any changes in scope, requirements, schedules, or cost in respect to the Ongoing Projects.

A.4.1.3 Resource Rationalization

Service Provider is responsible for the evaluation of customer demand and the rationalization of resources and coordination with DIR and DIR Customers to effectively meet competing demands of DIR Customers.

1. Provide DIR and DIR Customers with a report of the forecast of the demand queue by DIR Customer, projected resource requirements and resource constraints on a monthly basis.

2. Provide demand management in coordinate with DCS Service Providers, DIR and DIR Customer where resources and schedules are not in alignment.

3. Work with DIR Customer, DIR and DCS Service Providers to reprioritize projects based on Legislative mandates and currently committed resources in conformance to project management and prioritization processes in the Service Management Manual.

A.4.2 Quality Assurance

The goal of Quality Assurance is to maintain and gradually improve business-aligned IT service quality. As part of operating under an ITIL foundation, it is DIR’s expectation that Service Provider will employ a Quality Assurance (QA) program, tools, and repeatable processes and procedures to provide DIR and DIR Customers quality Services that are in accordance with the Service Level requirements as specified in **Exhibit 3**, Customer Satisfaction requirements as specified in **Exhibit 14** and are at a level consistent with acceptable industry practices and DIR current standards.

A.4.3 Operations Documentation

All documentation maintained by Service Provider will be subject to approval by DIR and DIR Customers and will conform to the documentation standards and format agreed upon between DIR and DIR Customers and Service Provider. Service Provider will develop documentation in accordance with the requirements in **Attachment 6-B**.

Service Provider’s responsibilities include:

1. Coordinate with DCS Service Providers to ensure that Service Component-specific operations documentation is up to date, accurate and posted in the Service Management Manual.
2. Develop and maintain documentation on all Operations procedures, services, Equipment, and Software for which Service Provider is responsible (e.g. project kick-off procedure, backup procedures, service desk scripts by agency, product ordering procedure, proposal formation procedure).
3. Document Application requirements that affect Operations, along with procedural information and contact information for each Application.
4. Make all documentation available in paper copies and electronically, as requested by DIR.
5. Validate documentation regularly for completeness and accuracy, and verify that all documentation is present, organized, readable, and updated.
6. Participate in the reporting of validation findings to DIR and DIR Customers on a regular basis, and where it is determined that documentation is inaccurate (e.g. erroneous or out of date), correct and replace such documentation.
7. Update the Service Management Manual according to the schedule described for the Critical Deliverables in **Attachment 3-C**.

A.4.4 Additions, Mergers and other Reorganizations

From time to time, DIR is required to and intends to, add or divest businesses (or parts of businesses), merge or split agencies, change its organizations or reorganize its business units. Service Provider will perform certain functions at the request of DIR or DIR Customers to support such activities.

Service Provider will conform to the requirements and provide the Services associated with business additions, mergers and other reorganizations as described in the MSA.

Service Provider's responsibilities include:

1. Assist DIR in planning, preparing and implementing any transition or changes related to the Services as a result of business additions, mergers or other reorganization (e.g. divestiture, acquisition, consolidation, relocation).
2. Where DIR has an existing commitment to provide IT-related services to a business reorganization, divestiture, acquisition, consolidation, or relocation, provide the required Services on behalf of DIR.
3. Develop and document processes and procedures to support business additions, mergers and other reorganizations.
4. Cooperate and coordinate with other DCS Service Providers and designated Third Party Vendors for the successful implementation of business additions, mergers and other reorganizations.
5. Perform all required changes associated with business additions, mergers and other reorganizations.
6. Perform all infrastructure changes as required.
7. Perform increased data and physical security as required.
8. Perform increased Disaster Recovery Planning and testing as required.
9. Implement business additions, mergers and other reorganizations in compliance with Project Management processes.
10. Actively support bringing additional DIR Customers into Services.
11. Provide proposals for transition and changes related to Services, in accordance with the Request Management processes.

A.4.4.1 Additional Customers

Service Provider's responsibilities include:

1. Describe Services to potential additional DIR Customers.
2. Provide proposals for transition to potential DIR Customers.
    2.1. Engage in activities relative to planning and developing solutions for proposals.
3. Add new users and organizations to its existing systems and tools (e.g. Portal) used to provide Services.
4. Add new sites and equipment into its existing system and tools (e.g. CMDB) used to provide Services.
5. Make changes to descriptors (e.g. name changes) associated with DIR and DIR Customers.

A.4.5 Crisis Management

Crisis management may be necessary depending on the type of business or geographic location where Services are being performed (e.g. hurricanes, tornados, riots, terrorist threats). Service Provider's responsibilities include:

1. Providing increase support when a crisis is declared.
2. Providing alternative communications methods (e.g. out of band communications support).
   - 2.1. Following statewide notification pyramid alert support as documented in the applicable business continuity plan.
   - 2.2. Following DIR notification processes for any crisis event occurring in or relating to a Service Provider Facility, DIR Facility or other facilities managed by Service Provider in connection with the Services.
3. Coordinating with DIR Customers, DIR and DCS Service Providers to implement Crisis procedures per the Service Management Manual.

A.4.6 Training and Education

Service Provider's responsibilities include the following:

1. Schedule and provide training on Service Provider Service Management Systems and other tools (e.g. Incident Management System, Configuration Management System), and the supporting processes to DCS Service Providers, DIR, DIR Customers and designated Third Party Vendors.
   - 1.1. Provide on-going methods for training as tools and processes are updated.

A.4.6.1 Training for New Authorized Users

Service Provider's responsibilities include the following:

1. Schedule and provide training on basic IT services for new Authorized Users, based on the needs of DIR or DIR Customers.
   - 1.1. Provide online training where it is the most effective delivery medium.
2. The content of the class will include but is not limited to the following:
   - 2.1. A general introduction to DIR's policies and procedures, and typical Equipment and Software for Authorized Users.
   - 2.2. User interface orientation.
   - 2.3. Network orientation.
   - 2.4. Data protection (backup and security).
   - 2.5. Network logon/off and general security procedures.
   - 2.6. Internet/intranet access.
   - 2.7. Passwords changes (as applicable).
   - 2.8. Access to Applications and communications.

2.9. Service Desk procedures and contact information.

2.10. Remote access procedures (as applicable).

A.4.6.2 Ongoing Training for Authorized Users

Service Provider's responsibilities include the following:

1. Continually investigate and analyze Authorized User training needs. Such analysis will be performed with the objectives of reducing the frequency of Calls to the Service Desk and preparing Authorized Users for the introduction of new technology and/or procedures.
2. Provide Authorized User training and associated documentation (e.g. user guide) for all Services.
3. Schedule and provide for individual products either on a requested basis or as a proactive step as part of an implementation project of a new technology /product.
4. Customize such training so that it is specific to the Authorized Users for the Services within the DIR environment.

   4.1. Provide multiple levels of training for specific Service Provider applications (e.g. beginner and intermediate training in standard applications used by Authorized Users and provided as part of Services).

   4.2. Provide training in the use of Equipment and/or Software that are used by Authorized Users (or that will be used as part of a new technology roll-out).

A.4.6.3 Training for Service Provider Personnel

Service Provider shall maintain documentation and training material for its own staff. At a minimum, Service Provider's responsibilities shall encompass:

1. Creating and maintaining Training material that includes at least the following information: the Services being provided, the value of these Services to DIR, the financial structure of charges, orientation and summaries on DIR and DIR Customers, DIR Security Policies, orientation to all applicable laws and regulations (e.g. TAC 202, HIIPA), the location of document stores, and the structure and location of the Service Management Manual.
2. Satisfying DIR that all Training material meets the minimum requirements for preparing Service Provider staff to support the delivery of Services, and engaging in updates of Training material shown to be deficient within designated timeframes.
3. Providing that all staff interacting with DIR or DIR Customers have reviewed the minimum set of documentation.
4. Reporting on the effectiveness of such training and the metrics associated with each staff that received training.
5. Upon request Service Provider shall provide such documentation and training to DIR and Third Party Vendors as specified by DIR.

A.4.7 Portal

DIR expects that Service Provider will support, enhance and maintain the existing Portal to be used as the centralized point of access to all documentation and information pertaining to the delivery of the Services, for Service Providers and other designated Third Party Vendors.

Service Provider's responsibilities include:

1. Design and implement a Portal that will be the centralized point of access to all documentation and information pertaining to the delivery of the Service, for Service Providers and other designated Third Party Vendors.
    1.1. Obtain the approval of DIR for the Portal integration and implementation plan.
    1.2. Ensure that the Portal integration and information formats are compliant with other portal technology standards and viewable by all stakeholders (e.g. web site, reports, etc.)
    1.3. Provide that the portal will allow users to login only once to access all portal functionality and provide a secure single point of access validation to associated systems (e.g. single-sign-on).
    1.4. Provide for secure access to information by DIR Customer, by Authorized User, and per DIR guidelines as specified in the Service Management Manual.
    1.5. Ensure that the Portal carries the approved DIR Brand.
2. Ensure that the Portal contains, at a minimum:
    2.1. Service Provider contact information.
    2.2. Online access to the Agreement, the MSA and all supporting documentation.
    2.3. Online access to Service Management Manual and any other operational agreements.
    2.4. Capability for DIR Customers to receive notification when special reports (e.g. root cause, low volumes of storage) are available on the Portal.
    2.5. Secure access for DIR Customers for view and access of DIR Customer specific information, which cannot be visible to other DIR Customers.
    2.6. Access to view, and the ability to download reports, as appropriate for all applicable customer reports for Services, by DIR Customer and with summary level reports for DIR.
    2.7. Access to the Chargeback System with agency-level and summary-level reports.
    2.8. Access to all applicable SLA reports.
    2.9. Access to all systems for the management of Services (e.g. Problem Management System, Change Management Systems).
    2.10. Access to calendar containing important schedules and dates including Governance meetings and Billing Invoice Dates, at a level of detail as required by DIR.
    2.11. Access to training materials on all of Service Provider's Services, Applications and operational systems that DIR Customers utilize (e.g. Billing Systems).

2.12. Necessary forms with capability to complete and submit (e.g. Request for Solution form, request forms).

2.13. List of Current Major Projects, by DIR Customer.

2.14. Single Sign On interfaces with DCS Service Provider applications.

2.15. Service Catalog with capability to place orders or link to Third Party Vendors in accordance with DIR procurement policies and standards.

3. Provide for self-service administration of information related to billing for DIR Customers (e.g. cost centers, site information, customer contacts), as described in **Exhibit 4**.

4. Provide access to FAQs and standard knowledge base information available from support centers (e.g. the Service Desk, Incident Management, Problem Management) based on current patterns of problems reported.

5. Make other information, as mutually agreed upon during the Term, available through the Portal.

6. Test all user interfaces and output, and ensure that, at a minimum:

6.1. All Web based pages using HTML, XHTML, and/or CSS are validated using the appropriate W3C validation service (http://www.w3c.org/)

6.2. Section 508 compliance (with §1194.22 Web-based Intranet and Internet Information and Applications) is validated using appropriate DIR Standards.

6.3. Portal is validated using the "Test and Evaluation Tools" identified in the Technology Plan.

6.4. All pages are usable with the screen readers identified in the Technology Plan.

6.5. If Java is used, the Java applet uses the accessibility API defined by the language.

6.6. Links that trigger scripts continue to work when scripts are turned off or not supported.

6.7. Updating the Portal to comply with future laws and Rules as they are adopted, in accordance with the Change Management process.

7. Ensure that the Portal meets current Federal and State laws for Accessibility.

A.4.7.1 Document Data Store

Service Provider shall be responsible for providing tools and processes for the storage of account documentation, including the Service Management Manual, knowledge bases of Incident and Problem resolution workarounds, Training Material, FAQs, and similar documentation for their own organization as well as from other DCS Service Providers and designated Third Party Vendors as specified by DIR.

These tools, processes and procedures must provide for effective data sharing and profiling across other DCS Service Providers and Third Party Vendors, DIR Customers and DIR, as specified by DIR.

Service Provider’s responsibilities include:

1. Provide processes, procedures and tools for integration to the Document Data Store.

2. Implementing process and procedures for the storage of documentation, including the Service Management Manual, knowledge base of incident and problem resolution workarounds, Training Material, FAQs, and similar documentation for their own organization as well as specified by DIR.
3. Cooperate with other DCS Service Providers and Third Party Vendors, DIR Customers and DIR, as specified by DIR to facilitate effective data sharing and profiling.

A.4.8 Network Connectivity

Service Provider's responsibilities include:

1. Coordinate with the Network Component Provider for network connectivity within the Consolidated Data Centers for provision of the Services.
2. If Service Provider chooses to implement some portion of the Services in facilities outside of the Consolidated Data Centers (e.g. disaster recovery sites, service delivery centers, etc.), Service Provider shall provide the network connections from those locations to the Consolidated Data Centers.
3. Provide the network connections between the Consolidated Data Centers, where Service Provider has some portion of the Services that require connections between the Consolidated Data Centers (e.g. data replication for disaster recovery, backup to a remote location, etc.).
4. For the network connections provisioned by Service Provider as part of its solution:
    4.1. Manage and support the network connections (e.g. WAN circuits).

    4.2. Ensure there is adequate bandwidth to support the full use of Services.

    4.3. Coordinate with the Network Component Provider to ensure proper connectivity between Service Provider's transport and the Consolidated Data Centers LAN.

A.5 Hybrid Cloud Initiative (HCI)

Service Provider’s responsibilities include the following:

1. Implement and maintain a Marketplace to allow authorized users to select services in the public cloud and DCS’ private community cloud in the Consolidated Data Centers, review the pricing, and submit the order. Information required for provisioning the service will be passed to the SCP. Service Provider will receive order status information, billing and usage data, and pricing information from the SCP.
2. Implement and maintain a Data Quality Management system to enable better automation, normalization, and reconciliation of asset information. Service Provider will receive electronically discovered data from the SCP and DIR Customers.